**LINCOLN-DOUGLAS |** CDI 14' Starter Pack

**Resolved: The United States ought to prioritize the pursuit of national security objectives above the digital privacy of its citizens.**

**TABLE  OF  CONTENTS**

TABLE OF CONTENTS 2

TOPIC ANALYSIS BY DEMARCUS POWELL............................................................... 15

AFFIRMATIVE EVIDENCE ........................................................................................... 50

*DEFINITIONS 50*

DIGITAL SURVEILLANCE DEFINITION 50

*CIVIL LIBERTIES, PRIVACY, AND CONSTITUTIONAL RIGHTS 51*

NSA SURVEILLANCE IS LEGAL 51

SURVEILLANCE IS LEGAL AND DOESN'T VIOLATE PRIVACY 52

LOSS OF PRIVACY IS INEVITABLE BUT SURVEILLANCE ENSURES BENEFITS FROM THIS LOSS 53

NSA SURVEILLANCE ISN'T ANY WORSE FOR PRIVACY THAN HAVING A FACEBOOK ACCOUNT 54

PRIVACY CONCERNS ARE NOT JUSTIFIED 55

THE PROGRAM PREVENTS TERROR ATTACKS THAT PRESENT A BIGGER RISK TO FREEDOM 56

CIVIL LIBERTIES ARE WELL PROTECTED 57

*CYBERSECURITY 58*

OUR CYBER INFRASTRUCTURE IS AT ENORMOUS RISK OF ATTACK—CURRENT JURISPRUDENCE IS INSUFFICIENT TO ENSURE SAFETY 58

CURRENT LEGAL INSUFFICIENCIES HAMSTRING OUR CAPABILITIES TO PREVENT TERRORISM AND ENSURE CYBERSECURITY—LEGAL ACTION IS NECESSARY 59

*AMEND ECPA 62*

AMENDING THE ECPA IS KEY TO FACILITATING COOPERATION BETWEEN ISPS AND THE GOVERNMENT, WHICH IMPROVES NATIONAL SECURITY 62

*AMEND SCPA 64*

TITLE II OF THE ECPA (THE SCA) SHOULD BE AMENDED TO ALLOW THE NATIONAL SECURITY COMMUNITY TO ACCESS THREAT INFORMATION. 64

*AMEND FISA 66*

FISA SHOULD BE AMENDED 66

*BINARY SEARCHES 68*

BINARY SEARCHES CAN LIMIT THE VIOLATIONS OF PRIVACY. 68

*DEMOCRACY 69*

SURVEILLANCE DOESN'T UNDERMINE DEMOCRACY - IT HELPS ACTUALLY HELPS IT 69

*GOVERNMENT SECRECY 70*

SECRET GOVERNMENT PROGRAMS ARE NECESSARY AND EFFECTIVE 70

[EXPERTS WITH ACCESS TO SECRET INFORMATION PROVE IT WORKS 71](#_TOC_250104)

NSA LEGAL 72

[NSA PROGRAMS ARE LEGAL BUT INTERNAL SECURITY WAS TOO LAX. 72](#_TOC_250103)

SECURITY 73

[SURVEILLANCE IS NECESSARY TO PROTECT NATIONAL SECURITY. 73](#_TOC_250102)

[IT IS POSSIBLE TO PRESERVE NATIONAL SECURITY WHILE KEEPING BALANCED CONSTRAINTS ON SURVEILLANCE. 74](#_TOC_250101)

TERRORISM 75

[BIG DATA HELPS TO PREVENT TERRORISM 75](#_TOC_250100)

[NSA PROGRAMS HELP TO PREVENT FUTURE ATTACKS. 76](#_TOC_250099)

[DIGITAL SURVEILLANCE IS KEY TO SECURITY 77](#_TOC_250098)

[SURVEILLANCE PROGRAMS ARE CRITICAL COUNTERTERRORISM TOOLS. 78](#_TOC_250097)

[PROGRAMS HAVE ASSISTED THE INTELLIGENCE COMMUNITY TO CONNECT THE DOTS. 79](#_TOC_250096)

[SURVEILLANCE PROGRAMS ASSISTED IN THE CAPTURE OF NAJIBULLAH ZAZI 80](#_TOC_250095)

[NSA SURVEILLANCE PREVENTS TERRORISM 81](#_TOC_250094)

[NSA SURVEILLANCE HAS PREVENTED 50 ACTS OF TERRORISM 82](#_TOC_250093)

[DIGITABLE SURVEILLANCE IS NECESSARY FOR EFFECTIVE COUNTERROR EFFORTS 83](#_TOC_250092)

[THE DATA IS VERY HELPFUL TO INVESTIGATIONS 84](#_TOC_250091)

[SURVEILLANCE IS CRITICAL TO PREVENTING TERRORIST ATTACKS 85](#_TOC_250090)

[SURVEILLANCE EMPIRICALLY PREVENTS ATTACKS ON THE HOMELAND 86](#_TOC_250089)

[SURVEILLANCE IS THE LAST, BEST DEFENSE AGAINST TERRORISM 87](#_TOC_250088)

[SURVEILLANCE IS NEEDED TO PREVENT TERRORISM 88](#_TOC_250087)

[SURVEILLANCE PROVIDES INFORMATION TO PREVENT A FUTURE 9/11 89](#_TOC_250086)

[TERRORISM IS A REAL THREAT - SURVEILLANCE IS REQUIRED TO DEFEAT IT 90](#_TOC_250085)

[SURVEILLANCE WOULD HAVE PREVENTED 9/11 91](#_TOC_250084)

[ERR ON THE SIDE OF EXPANSIVE INTELLIGENCE PROGRAMS 92](#_TOC_250083)

[TERRORISTS WANT TO ATTACK THE US BUT SURVEILLANCE EFFORTS STOP THEM 93](#_TOC_250082)

[ABSENT NSA SURVEILLANCE, THERE WOULD HAVE BEEN MORE ATTEMPTED ATTACKS 94](#_TOC_250081)

[SURVEILLANCE SYSTEMS EXIST BECAUSE THEY WORK 95](#_TOC_250080)

AT ABUSE OF POWER 96

[THE NSA IS AN ACCOUNTABLE PROGRAM 96](#_TOC_250079)

[THERE ARE INTERNAL CHECKS ON PRIVACY LOSS 97](#_TOC_250078)

[SURVEILLANCE IS LAWFUL AND EFFECTIVE 98](#_TOC_250077)

[THERE IS NO EVIDENCE OF PROGRAM ABUSE 99](#_TOC_250076)

[ABUSE CONCERNS ARE ENTIRELY BASELESS 100](#_TOC_250075)

AT LEGALITY 101

[THERE IS LEGAL PRECEDENT FOR THE NSA’S ACTIONS. 101](#_TOC_250074)

[THE OBAMA ADMINISTRATION IS ON SECURE LEGAL FOOTING 102](#_TOC_250073)

[NSA SURVEILLANCE DOES NOT VIOLATE THE FOURTH AMENDMENT. 103](#_TOC_250072)

AT MOTIVES 104

[NSA SURVEILLANCE ISN’T BASED ON ULTERIOR MOTIVES. 104](#_TOC_250071)

AT TRANSPARENCY 105

[NEW NSA CHIEF WILL IMPROVE TRANSPARENCY. 105](#_TOC_250070)

[IMPROVED TRANSPARENCY WON’T HINDER THE NSA. 106](#_TOC_250069)

NEGATIVE EVIDENCE ............................................................................................... 107

DEFINITIONS 107

[PRIVACY DEFINITION 107](#_TOC_250068)

[PRIVACY INVOLVES PERSONAL AND PHYSICAL PRIVACY 108](#_TOC_250067)

[DIGITAL PRIVACY DEFINITION 109](#_TOC_250066)

[ORGANIZATIONAL PRIVACY DEFINITION 110](#_TOC_250065)

[PRIVACY DEFINITION 111](#_TOC_250064)

ABUSE OF POWER 112

[PROGRAM ABUSE HAS HAPPENED BEFORE AND WILL CONTINUE 112](#_TOC_250063)

[PROGRAM ABUSE IS INEVITABLE 113](#_TOC_250062)

[SURVEILLANCE INEVITABLY BLEEDS INTO DISCRIMINATION AND PROFILING 114](#_TOC_250061)

CANADA 115

[CANADA AIDS THE NSA IN SURVEILLANCE. 115](#_TOC_250060)

[THE NSA BRIBES CANADA FOR ASSISTANCE IN SURVEILLANCE. 116](#_TOC_250059)

CIVIL LIBERTIES 117

[NSA SURVEILLANCE VIOLATES CIVIL LIBERTIES. 117](#_TOC_250058)

[THERE ARE FOUR WAYS THAT DIGITAL SURVILLANCE VIOLATES PRIVACY. 118](#_TOC_250057)

[LIBERAL DEMOCRACY DEMANDS THE RIGHT TO PRIVACY 119](#_TOC_250056)

COST 120

[NSA PROGRAMS ARE OUTRAGEOUSLY EXPENSIVE. 120](#_TOC_250055)

[THE NUMBER OF AL QAEDA OPERATIVES IN THE US DOES NOT JUSTIFY THE DOLLARS SPENT ON SURVEILLANCE. 121](#_TOC_250054)

DEMOCRATIC FREEDOMS 122

[SURVEILLANCE HAS A CHILLING EFFECT ON ALL DEMOCRATIC FREEDOMS 122](#_TOC_250053)

[SURVEILLANCE CREATES A CULTURE OF FEAR AND DISTRUST 123](#_TOC_250052)

[SURVEILLANCE DESTROYS ACCOUNTABLE DEMOCRACY AND PRIVACY 124](#_TOC_250051)

[NSA SURVEILLANCE IS THE DEATH KNELL FOR DEMOCRACY 125](#_TOC_250050)

[OPEN, FREE TECHNOLOGY IS NECESSARY TO BE AN ENGAGED CITIZEN 126](#_TOC_250049)

[SURVEILLANCE STIFLES INDIVIDUAL INNOVATION AND FREE THOUGHT 127](#_TOC_250048)

[SURVEILLANCE CONSTRAINS FREEDOM OF INNOVATION AND EXPERIMENTATION 128](#_TOC_250047)

[SURVEILLANCE UNDERMINES RIGHTS TO FREE SPEECH AND PRIVACY 129](#_TOC_250046)

[SURVEILLANCE INEVITABLY DETERS TRULY FREE SPEECH 130](#_TOC_250045)

IMMIGRATION 131

[VIOLATION OF DIGITAL PRIVACY CAN LEAD TO WRONGFUL DETAINMENT. 131](#_TOC_250044)

[NSA SURVEILLANCE DISPROPORTIONATELY AFFECTS IMMIGRANTS 132](#_TOC_250043)

LEGALITY 133

[NSA SURVEILLANCE VIOLATES THE CONSTITUTION. 133](#_TOC_250042)

[THE US SUPREME COURT HAS RULED AGAINST VIOLATIONS OF PRIVACY ON THE FOURTH AMENDMENT 134](#_TOC_250041)

[NSA SURVEILLANCE IS ILLEGAL 135](#_TOC_250040)

[NSA SURVEILLANCE VIOLATES THE FOURTH AMENDMENT 136](#_TOC_250039)

[NSA SURVEILLANCE IS AN UNACCEPTABLE INFRINGEMENT OF THE 4TH AMENDMENT 137](#_TOC_250038)

[SURVEILLANCE VIOLATES CONSTITUTIONAL GUARANTEES OF INTELLECTUAL FREEDOM 138](#_TOC_250037)

[THE SURVEILLANCE AUTHORITY CLAIMED BY THE NSA IS SWEEPING AND OVERBROAD 139](#_TOC_250036)

[THE GOVERNMENT ARGUES THAT AMERICANS HAVE ESSENTIALLY NO REASONABLE EXPECTATION OF PRIVACY IN ELECTRONIC COMMUNICATIONS 140](#_TOC_250035)

LEGISLATION 141

[THE HOUSE RECENTLY PASSED A BILL TO LIMIT NSA SURVEILLANCE. 141](#_TOC_250034)

[NEW ATTEMPTS TO REGULATE NSA SURVEILLANCE ARE BEING WATERED DOWN 142](#_TOC_250033)

[THE USA FREEDOM ACT WILL INCLUDE NEW RESTRICTIONS ON NSA DATA STORAGE 143](#_TOC_250032)

[THE USA FREEDOM ACT HAS GOTTEN WEAKER AND WEAKER OVER TIME 144](#_TOC_250031)

NSA ACTIVITIES 145

[THE NSA COLLECTS DATA THROUGH PRIVATE TELECOMMUNICATIONS AND INTERNET SERVICE PROVIDERS 145](#_TOC_250030)

[THE NSA CAN TRACK EVERY KEYSTROKE ON A COMPUTER. 146](#_TOC_250029)

[THERE ARE NUMEROUS TECHNIQUES TO BREACH DATABASE SECURITY. 147](#_TOC_250028)

PRIVACY 148

[SURVEILLANCE IS A DIRECT ASSAULT ON PRIVACY. 148](#_TOC_250027)

[NSA ACTIONS ARE EGREGIOUS VIOLATIONS OF PRIVACY. 149](#_TOC_250026)

[NSA SURVEILLANCE UNDERMINES OUR BASIC RIGHT TO PRIVACY 150](#_TOC_250025)

[THE PROGRAM IS A MASSIVE INVASION OF PRIVACY 151](#_TOC_250024)

[MISTAKES THAT CAUSE ABUSE AND INVASIONS OF PRIVACY ARE INEVITABLE 152](#_TOC_250023)

ROUTERS 153

[THE NSA IMPLANTS ROUTERS WITH SURVEILLANCE TOOLS TO FACILITATE SPYING ON INTERNATIONAL USERS 153](#_TOC_250022)

[THIS TYPE OF INVASION OF PRIVACY IS EXACTLY WHAT THE US HAS ACCUSED CHINA OF IN THE PAST. 154](#_TOC_250021)

SCOPE 155

[THE SCOPE OF NSA SURVEILLANCE EXCEEDS ITS ABILITY TO ANALYZE IT. 155](#_TOC_250020)

[THE NSA HAS ADMITTED THAT IT COLLECTS MUCH MORE DATA THAN IT CAN ANALYZE. 156](#_TOC_250019)

SOFT POWER 157

[NSA SURVEILLANCE DEVASTATES OUR INTERNATIONAL CREDIBILITY 157](#_TOC_250018)

[SURVEILLANCE JUSTIFIES AUTHORITARIAN CRACKDOWNS AROUND THE WORLD 158](#_TOC_250017)

SURVEILLANCE STATE 159

[THE INTERNET HAS BECOME A SURVEILLANCE STATE 159](#_TOC_250016)

TECH INDUSTRY 161

[SURVEILLANCE THAT UNDERMINES PRIVACY HURTS THE TECH INDUSTRY 161](#_TOC_250015)

AT TERRORISM 162

[NSA SURVEILLANCE IS NOT INSTRUMENTAL IN DISRUPTING TERRORIST PLOTS. 162](#_TOC_250014)

[CASE STUDIES INDICATE NSA PROGRAMS WERE NOT IMPORTANT. 163](#_TOC_250013)

[DATA MINING WON’T WORK WITH TERRORISM 164](#_TOC_250012)

[SIMPLE TOOLS ARE MORE EFFECTIVE FOR COUNTERRORISM 165](#_TOC_250011)

[THERE'S NO EVIDENCE THE PROGRAM IS EFFECTIVE 166](#_TOC_250010)

[THE PROGRAM IS INEFFECTIVE AND UNDERMINES DEMOCRACY 167](#_TOC_250009)

[THE PROGRAM ISN'T NECESSARY TO STOP TERRORISM 168](#_TOC_250008)

[THE PROGRAM HAS NOT PREVENTED ANY ATTACKS 169](#_TOC_250007)

[ATTACKS THAT HAVE BEEN PREVENTED WEREN'T BECAUSE OF THE NSA 170](#_TOC_250006)

[TERRORIST ATTACKS CAN BE PREVENTED OTHER WAYS 171](#_TOC_250005)

[EMPIRICAL EXAMPLES PROVE THE PROGRAM IS NOT BENEFICIAL 172](#_TOC_250004)

[TERRORISTS ARE ADAPTING TO AVOID SURVEILLANCE 173](#_TOC_250003)

[THE PROGRAM IS A HUGE WASTE OF TAX DOLLARS 174](#_TOC_250002)

AT TIPS 175

[THE TIPS PROGRAM WILL MAKE US A NATION OF SUSPECTS. 175](#_TOC_250001)

[TIPS IS ESSENTIALLY HIGH-TECH MCCARTHYISM 176](#_TOC_250000)

**Topic  Analysis  by  Demarcus Powell**

.

There are some words in the resolution that will be important for the development of both good and bad arguments:

*Prioritize*

The meaning of the word is pretty clear -- that is, to prioritize is to treat as more important. There are a couple of problematic arguments that will arise out of this.

First, debaters on both sides of the resolution will try to avoid engaging the core questions of the topic by asserting that “prioritizing A over B doesn’t mean you don’t also value B.” They will use this argument as a tool to get out of any impact the opponent proposes. For example, if the negative argues that the aff denies freedom because it undercuts digital privacy, the aff will say, “Look, I don’t harm digital privacy. I’m just arguing that security is more important, not that we shouldn’t *have* digital privacy.”

The stock interpretation of topics like this is that the two values under discussion are in conflict or tension and that, under the circumstances proposed by the resolution, governments have to make a choice between them. Thus, prioritizing “national security objectives” over “digital privacy” means that digital privacy will be lost, violated, undercut, whatever.

The go-to strategy for people who want to avoid debating the difficult questions of a resolution is to try to find (usually semantic) ways to avoid bearing the burden of defending their side of the topic. So debaters will absolutely extend their definition of “prioritize” to mean that the state is still *valuing both,* because both are in the list of priorities, so whatever impact you are talking about simply won’t happen, because they don’t have to defend *eliminating* the value represented by the other side of the topic.

Another strategy that operates along the same lines, but typically only available to the negative, is the *balance position.* A balance position is really simple and a surprisingly broad cross-section of debaters and coaches think that it is actually a good idea. The balance position just says that the two values posited by the resolution have identical value -- they can’t be prioritized because they are both equally good (or bad.)

One thing that the wording committee sometimes does to avoid this problem is to introduce a phrase like “when in conflict,” to indicate that the two values in the resolution can’t be balanced, and also that each debater has to defend not just the “goodness” of one value but the implications of pursuing that value at the expense of the other. The prevalence of “when in conflict” phrases actually matters here because the very *absence* of such a phrase will make these kinds of squirrelly strategies all the more common. Coaches will figure, “Well, since they didn’t include ‘when in conflict,’ they must have intended the balance position to be neg ground.”

These kinds of positions are deeply harmful to debate because their *only* purpose is to avoid the central question of the topic. If you’ve come to debate, then just accept the burden implied by your side and prove it.

To be clear: the stock aff is *it’s OK to violate digital privacy in order to maintain national security,* while the stock neg is *digital privacy is sufficiently important that it cannot be violated, even if doing so is necessary to achieve national security.* Give or take solvency arguments on both sides, those are the burdens that a straightforward debater should accept and defend.

*National Security Objectives*

This term is fascinatingly ambiguous. First, the value isn’t *national security,* but *objectives.*

Objectives are goals. So this raises a couple of questions:

1) Are national security objectives guaranteed to be connected to actual national security? It’s possible that unwise leaders pursue certain goals in the *name* of national security that actually have no rational connection to national security. The affirmative cannot simply assume that the two concepts are identical. That means that “national security objectives are ephemeral and vague” is neg ground. The affirmative can avoid getting bogged down in this debate by carefully defining the range of national security objectives they are defending, or by forwarding good arguments in the AC framework that show that national security objectives are *actually* important.

2) Is there any guarantee that, given quality objectives, violations of digital privacy can achieve them? In other words, solvency arguments are negative ground (at least potentially.)

This gets at an important distinction in approaches to the topic. On the one hand, the aff might say that they are approaching the topic purely as a question of value. Which of the two concepts -

- national security or digital privacy -- is more valuable, innately? Given this interpretation, it doesn’t particularly matter what the policy implications of affirming are. The affirmative will argue that value decisions precede policy decisions, and that this resolution poses the value question,

not the policy question. So, once we determine that national security *is more important* than digital privacy, we have to make subsequent policy determinations, but those questions are for another round. Today we’re just answering the question of which value is more important.

This interpretation excludes solvency or other policy-style arguments. But it also precludes the affirmative from making ends-based arguments about how violations of digital privacy are key to solving terrorism and other national security threats. And those are potentially very persuasive arguments.

The second interpretive approach is the policy-esque approach. The affirmative treats the resolution more or less as a plan, and advocates a government policy (which could be general or very specific) of violating digital privacy rights in order to protect national security. Here the affirmative can read evidence about how FBI, CIA and NSA digital snooping has successfully foiled some number of terrorist attacks, protecting American lives in the process.

The advantage to the affirmative of the second approach is that, especially given a diverse judging pool, concrete arguments about tangible benefits are going to be very persuasive. The drawback, of course, is that it opens the affirmative up to negative arguments that digital snooping doesn’t protect national security (solvency arguments) and arguments that digital snooping creates other problems (disadvantages.)

If you are going to go with the second interpretation, which treats the resolution more-or-less as a policy position, then you should be careful in how you write your cases. There are a lot of judges at nationals who are very committed to the old-school idea that LD and policy debate are very distinct activities. They will still accept ends-based argumentation as long as it is presented with a tasty candy coating of values and criteria, and as long as you avoid as much as possible those nasty policy buzzwords like “solvency” and “disad.” On the other hand, some judges at nationals don’t mind those things at all. One option is to have two versions of a case -- one written with policy structure and jargon, and one shoe-horned into the traditional LD format. Think “Value of justice, criterion of utilitarianism.”

Another issue with the phrase “national security” is the scope of harm implied by its violation. Affirmative debaters are going to want to exaggerate that scope as much as possible -- to the aff, a loss of national security means doom, I say, **DOOM!** for the nation. Not only will everyone die but they’ll be roasted on spits and turned into petit-fours. To the negative, national security is much less clearly-delineated and vastly less dire. A loss of national security might lead to a rival nation finding out, for example, the First Lady’s secret banana bread recipe. Or something. The

point is, if “national security” implies dire and immediate consequences, it is much easier to argue that we ought to subvert digital privacy in its service. After all, your digital privacy doesn’t matter if you’re the victim of a thermonuclear attack! On the other hand, if (as is more probably the case), “national security objectives” are relatively picayune matters overseen by partisan politicians and marginally competent bureaucrats, it’s very difficult to justify wholesale violations of digital privacy rights. This will be a matter for both the definition level of the case and for substantive argumentation within the case.

*Digital privacy*

This is a term of relatively recent coinage. The closest thing you’ll find to a “definition” of the phrase is something like, “a right of privacy relating to information stored in digital media or transmitted digitally, i.e. over the internet.” Once again, however, you can choose to define the concept very broadly or very narrowly. In this case, the affirmative has an incentive to define the term narrowly -- the less that is covered by “digital privacy,” the easier it is to justify violations. The aff probably cannot limit the concept down farther than “information stored on your computer” but other questions remain: does digital privacy include information stored in “the cloud” -- which is basically just a metaphor for information stored, on your behalf, on a server that exists in a location other than your home or work? Does digital privacy cover digital communications over phone and fax lines, or only computer lines? Does it cover the information contained in your car’s computer, your GPS system, your phone, your tablet, etc. -- especially now that most of these devices can track your movements? Also, there are ways that a savvy computery-hackery-type person can remotely turn on the little camera that now comes standard on all laptop and desktop computers, so they can literally spy on your movements in your home. (And this is *not* far-fetched

-- a number of cases have turned up in the last five or six years where authority figures of one stripe or another have done *exactly this.)* Does digital privacy cover *that?* After all, in the case of computer-camera snooping, the *means* of snooping is digital (that is, the information transmitted by the camera is compressed into a digital format) but the information gathered (images of you moving around in your home, audio of same) is not digitally stored. What about digitally stored medical records?

If you take a very broad view of digital privacy, it’s easy to argue that our entire lives have been so thoroughly digitized that digital privacy is *the fundamental* form of privacy. If the government can violate our digital privacy at will, they can find out literally everything about us. Not just what we voluntarily put on Facebook, but our movements (tracked by our phones), our private lives, our medical secrets, our educational records -- everything. It’s like that machine that Bruce Wayne built in the last *Batman* movie -- digital technology is so pervasive in our society that a true absence of digital privacy would give authority figures almost godlike power to monitor us.

The affirmative wants to have a reasonable, but narrower, definition of “digital privacy.” A good aff definition might restrict digital privacy to privacy covering that information that a person voluntarily stores in a digital medium (i.e. on their computer or on the cloud). That would limit out some of the other, more obviously egregious forms of digital snooping. But, again, the range of possible meanings of “digital privacy” is going to be subject of both definitional and substantive debate.

There is one other interesting concern about the word “privacy.” By itself, it is a controversial term in constitutional law. In particular, the scope of privacy is a hotly contested question. One definition often offered to explain the difference between private and non-private information is that private information is shared in circumstances where one has a reasonable expectation that others are not observing them, while any information shared under circumstances where there is *no* reasonable expectation that others are not observing is not private. For instance, if I call my wife my “Snuggley Poo” in our own home, and someone is listening at the window, their observation of my term of endearment is a violation of privacy. But if I call my wife “Snuggley Poo” in the middle of a crowded Wal-Mart, I can’t claim a privacy violation when someone overhears.

Based on this definition, some might argue that there is no such thing as “digital privacy,” since the ability to monitor digital media is so widely available (and so well-known) that anyone who publishes any information digitally can’t reasonably expect that others will not observe. If you send something out into the world in the form of an email or Facebook post, or even if you store some documents on a cloud server, you have to know that *someone* is going to be able to observe those things. Since there is no reasonable expectation that your digital transmissions will not be observed, there is no such thing as “digital privacy.”

Of course, this definition of “privacy” breaks down at some point. Consider the prototypical private situation: you and your significant other in the privacy of your bedroom. No one would object to the idea that information you share behind closed doors and curtains is absolutely private. But say, at some point in the future, that someone develops technology that makes it easy to scan through solid walls to take detailed photos, video and audio. Say this technology becomes inexpensive and widely available. Now anyone with a few bucks can go down to the Best Buy (because they’ll still exist, of course) and purchase a Spy-O-Tron 3000. In this world, you no longer have a reasonable expectation that your activities in the bedroom will go unobserved because with the good ol’ Spy-O-Tron, your bedroom walls are as clear as glass. Would you then say that someone who records your activities with the Spy-O-Tron is *not* violating your privacy?

Obviously not. They totally are. There must be some basic conception of privacy that exists

absolutely and is not subject to the “reasonable expectation” test.

One final note on topic analysis: The resolution doesn’t specify the method by which digital privacy might be subverted to the needs of national security. The “current controversy” most closely associated with this topic is the use by the government of shady, warrantless data collection programs -- the kind of thing Edward Snowden alerted us to before he deserted to Russia, the rat fink. The aspect of these programs that people find most troubling is not *just* that they subvert privacy to national security, but that they do it in an unwarranted way -- that is, the people who gather phone numbers or peer at private internet pages or tap phone lines can do so without seeking any permission from a judge or other authority. Our society has a fairly well- established principle that as long as authorities can show some reasonable cause for a search, it’s okay to violate privacy. We draw an important distinction between warranted and unwarranted searches. But that doesn’t mean that a *warranted* search isn’t still a violation of privacy. I think the affirmative can make the argument that since the resolution specifies that the value of digital privacy is in competition with *national security concerns,* the policy implication of the resolution is that the aff defends digital surveillance based on some kind of reasonable suspicion or warrant. A truly warrantless search, the aff might argue, doesn’t respond to any actual concern -- it is arbitrary for exactly that reason.

This bit of resolutional analysis puts the negative in a potentially tough spot. The sense-making response to this observation is that so-called “warrantless” information gathering actually does have a reason behind it -- specifically, that large-scale analysis of “meta data” is the only way to spot evidence of impending terror attacks prior to the attack actually happening. Because terrorists take great pains to avoid arousing suspicion, the standard justification of “reasonable suspicion” is too limiting for these kinds of searches to be effective. This is why there is an actual conflict between digital privacy and national security concerns, even if there is no suspicion regarding the privacy of the particular person. This analysis explains why the previous argument is wrong -- that is, it explains why a national security concern can arise even in the absence of particularized suspicion. But in doing so, this argument also seems to go a long way toward explaining why violations of digital privacy are key to stopping terrorism.

Perhaps this question of warranted versus unwarranted digital monitoring won’t even come up. But I think it will pay to spend some time thinking about what you’re prepared to advocate for on both sides.

AFF ARGUMENTS

To start off with, I think the aff would benefit from a framing argument that points out that affirming doesn’t justify *warrantless* privacy violations, a la the recent NSA phone-records scandal; or, at the very least, that it doesn’t justify *solely* warrantless

The most basic affirmative argument is ends-based and very simple: the government’s ability to access digital information is vitally important. Terrorists are very careful in their plotting and planning, and they are smart enough that they can hide their plans from the authorities. However, terrorists and other evil-doers are highly dependent on modern communication technology, including computers, the internet, and cell phones. That means that a carefully constructed system of digital monitoring can successfully spot terror attacks *before* they happen. You might point out the important distinction between proactive and reactive responses to terrorism: without digital monitoring, the authorities can be *reactive* to terror attacks, meaning they can go after the perpetrators after the crime has been committed. But in terms of national security, that is not really sufficient, because national security breaches -- like 9/11 -- have tremendous short-term costs. We can’t afford to wait until after the event to react.

You can approach the efficacy or solvency debate from one or both of two perspectives: you can explain *why* digital monitoring is an effective tool against terrorism, and you can present evidence that such monitoring actually has led to the arrest of terrorists and/or to the avoidance of terror attacks. The latter kind of evidence is somewhat hard to come by, largely because of the secrecy involved in these matters -- the people in charge of using covert monitoring to foil terror plots cannot put out press releases trumpeting their successes. Some of the evidence makes the point that, since 9/11, there hasn’t been a successful large-scale terror attack in the US, but absence of such an attack hardly proves that digital monitoring is vital to the prevention of attacks. The evidence you’re looking for is going to specify how covert digital monitoring has foiled specific attacks under specific circumstances.

A more value-oriented approach might be easier to prove. One argument you might forward is that, at base, “national security” is a more fundamental value than “digital privacy.” Nations exist in a competitive and hostile environment, so the concept of “national security” is not just some vague bureaucratic notion. Nations, particularly powerful ones like the United States, have enemies who actively seek to do large-scale harm. Even countries that we consider more-or-less allies, like China, are engaged regularly in electronic attacks against our infrastructure. The competition between major powers over access to resources and regional dominance is very real. Each country, therefore, has a need to maintain a national security system, without which other countries could and would overthrow or otherwise do harm to us. And, in a world where weapons of mass destruction such as nuclear weapons and biological weapons can be miniaturized and

transported easily, that damage could well be existential in nature. Put simply: the stakes for national security are as high as they can be. Without national security, the lives of not just some but potentially *all* Americans could be at risk. That means that “national security” is a prerequisite to all other values because, as is commonly pointed out, other values, privacy included, aren’t worth much if you’re dead.

This argument has to overcome some inertia. Our society has been pelted with talk about “national security” for, seemingly, *ever,* and it has only gotten worse since the 9/11 attacks of 2001. There is a strong sense, particularly among political liberals and libertarians, that “national security” is a euphemistic justification for a more controlling, autocratic government that seeks not to protect the nation, but rather to expand its own power, at the expense of civil liberties such as privacy. People have grown cynical regarding “national security” threats. If you simply refer to “national security” in your cases as though it were a given that we would *all die* without it, your argument will be less persuasive.

Digital privacy is unimportant.

In the strict offense/defense sense, arguments that digital privacy is relatively unimportant are not “offense” because they are not reasons to reject digital privacy, nor are they directly comparative with national security. However, since the resolution is a comparison of values, arguments that undercut both the philosophical/value-based importance of digital privacy and the scope of policy implications regarding digital privacy can be persuasive. Generally speaking they tell the judges that digital privacy is not really a big concern, and (coupled with reasons why national security *is* a big concern) they can form the basis of a strong strategy at NSDA nationals. So, here are a number of arguments that undercut the importance of digital privacy:

First, “privacy” is not a constitutional principle in the United States. It is a “penumbral right,” meaning that the Supreme Court has interpreted other constitutional principles as extending to create a right of privacy, but privacy, by itself, is not mentioned in the Constitution. On the other hand, the obligation of the government to maintain the collective security of the state is deeply rooted in the founding documents. Extending the literalist interpretation of the Constitution further, it is certainly the case that the framers did not intend to create laws protecting *digital* privacy, since such a thing was not imagined in their time.

People can manage digital privacy. Believe it or not, there was a time before computers when people communicated with things like “conversations” and, if they were separated by enough distance that conversations were inconvenient, “letters.” Participation in the digital world is entirely voluntary. People can manage their participation in digital communications and use of

digital media to minimize or eliminate the implications of digital privacy violations. If you don’t

want other people to know it, don’t send it in an email.

Further, teaching people (especially children) not to rely on digital privacy is beneficial. Regardless of what the government does, there are all kinds of hackers and stalkers and criminals of various stripes who are apt to steal your emails, clone your cell phones, download your credit card data, etc. We should absolutely be treating digital media and communications as untrustworthy. If people behave appropriately toward the internet, then government snooping shouldn’t matter.

Digital privacy violations are macro-level, not micro-level, and so don’t meaningfully intrude. The media reports about the NSA’s various digital surveillance programs have not made it clear exactly what kind of digital media are being snooped and how. The media report that the government is “monitoring our phone calls” and people imagine an NSA spook sitting there listening to your dirty conversations with your girlfriend. That’s nonsense. The government has neither resources nor inclination to monitor personal communications without warrant. What the government does under various NSA programs is to aggregate “meta data” -- not phone calls themselves, for instance, but information *about* phone calls, i.e. phone bill data. The number of calls made, the numbers called, the duration of calls, and so forth. This data can be mined to try to find trends or signs of untoward behavior, which can be used to catch terrorists and stop plots. But the nature of the information is not highly personal, at least not in the sense that people imagine when someone tells them that the government is “monitoring phone calls.”

Checks and balances exist to prevent abuses of digital monitoring systems. Remember that, while the controversy over NSA spying centered on the unwarranted nature of the programs involved, the resolution doesn’t specify whether privacy violations by the government are or are not subject to requirements of reasonable suspicion. There are checks and balances in place to prevent abuses of power in the area of digital privacy. First, agencies that violate digital privacy are required to submit their searches to courts to obtain a warrant. Even where there are programs that do *not* require this kind of warranting, there are political checks and balances. Since Washington politics is highly polarized and competitive, each party has an incentive to keep the other party in check. When George Bush instituted warrantless wiretapping on the sly, Democrats made sure that everyone knew about it. Under Obama, NSA surveillance was brought to the fore, initially by Edward Snowden, and then by Obama’s political enemies.

Privacy is a classist concept -- we should deprioritize it. I don’t think you’ll see this argument much at nationals, but I’m sure *someone* will run it. The critique of privacy points out that the

amount of privacy we enjoy is correlated with our wealth. Wealthy people live in single family homes in relatively low-concentration areas, while poorer people live in highly concentrated environments in smaller, multi-family units where they share walls and hallways with other families. For this and other reasons, privacy is not a universal value enjoyed equally by all, but rather just another example of the privileges of wealth. That means we should deprioritize privacy so as to maintain equity.

Social contract and/or communitarian approach. This argument is, I think, one of the better ones. There are a couple of points to this argument. The first is that we exist in a communal order that has to be protected. We have to be willing to sacrifice certain individual rights where necessary to maintain that social order. If we accept the benefits of living in a shared social order but then reject the burdens, we are violating the contract. The fact that the resolution places privacy in conflict with *national security* makes this argument particularly pertinent, because it is the survival of the social order writ large that is at risk in this conflict. Second, as long as those sacrifices are equitably, no one really has a reason to complain. There is no such thing as an absolute right -- all rights are subject to some degree of limitation. Less relevant than the degree of limitation of a given right is the equity in distribution of limitations. If we are all limited in the same way, then, first, that is fair, as no one is treated differently based on arbitrary characteristics. And, second, there is an inherent check on the degree of rights violation -- since the violations apply to everyone equally, if the violation goes farther than is tolerable, then people will react to undo the system of rights violations. From the communitarian perspective, limitations of individual rights are only dangerous to the extent that they express privilege -- leaving the rights of some intact while others bear disproportionate burdens.

A liberal-rights argument in favor of digital monitoring might point out that we simply don’t have a right to maintain “dangerous secrets.” The right to privacy is important, but the right to privacy can’t trump the right of others to safety. For instance, I don’t have a right to keep dynamite in the closet of my apartment, because doing so creates a danger to others, and I don’t have a right to create that danger. If we live in a system in which bad actors can use digital storage and communications to plan and carry out bad acts, and if it is the case that the only way that the government can detect and prevent these bad acts is to monitor digital storage and communications, then insisting that our privacy be respected fails to consider the welfare of others. Each person may have an individual incentive to insist on digital privacy -- since terror attacks are rare, the probability that a terror attack will affect *you* is very low. So it seems like a good deal, from your own perspective, to allow the risk of terror attacks to increase slightly in order to obtain some digital privacy benefit for yourself. After all, even though this drives up the probability of terror attacks, the attack will almost certain affect someone else, who you don’t

know. So from your own perspective it makes sense to trade some digital privacy against an attack that will kill some anonymous other. But this is clearly a violation of morality -- your willingness to sacrifice an anonymous other in return for a relatively trivial personal right fails to respect the moral equality of the anonymous other. If I told you that you needed to give up digital privacy or there would certainly be a terror attack that would *affect you, or someone close to you,* you would (assuming you believed me) be willing to give up the digital privacy. It is immoral to fail to accord the same respect to an anonymous other.

NEG ARGUMENTS

Freedom is the reason America is a valuable country. To begin with, it’s important to make the case that there are some values that cannot be sacrificed even in the name of national security. The United States was created to enshrine freedom; if we can only preserve the United States through wholesale violations of freedom, then perhaps it is not worth preserving in the first place. Now certainly, there are other ways to protect our national security that don’t involve widespread violations of freedom, but still, we should not orient ourselves to accept freedom violations in the name of security.

Digital privacy violations don’t work. There’s no evidence that any terror attacks have been stopped. This is an obviously empirical point, but there is good evidence to support it. It is probably the case that the reason there is so little evidence to support the notion that terror attacks have been stopped thanks to digital privacy is that the organizations engaged in these activities have to operate in secret, but, still, it seems that there should be *some* evidence of significant security benefits in exchange for the vast violations of digital privacy that have been undertaken by the US government.

You might make the argument that digital privacy violations don’t work because terror networks are too savvy to communicate in ways that can be overheard by the government. You can make the further argument that even if it *was* the case that digital privacy violations were effective *prior* to Edward Snowden’s famous leaks, it is *no longer* the case because now that the whole world knows that the NSA is eavesdropping on everyone’s computer communications and phone calls, terrorists will have adapted. So even if in principle it’s justifiable to violate privacy *in the name of security,* it is simply no longer the case that that principle applies, thanks to the news developments of the past year. The digital privacy cat is out of the bag, so to speak.

Secretive powers inherently undermine democracy because they are by their very nature uncheckable. Government has to be accountable to the people in order for democratic systems to function. The only reason that state power is justified in a liberal democratic framework at all is

that the people are given the power to evaluate the actions of the government officials and vote them out of office as they see fit. If the government is able to operate in secret, then democracy simply can’t function -- no matter what the government does, no matter how terrible, the check of the democratic vote can’t function if the government has the power to keep it secret. And digital privacy violations only make sense to the extent that they operate in secret -- if the government has to let everyone know what communications are being monitored and how, then there’s no way they’ll every find anything out. So, digital privacy violations are simply incompatible with democratic governance.

Privacy is a very important value -- it’s key to freedom. At camp last summer, I saw a lot of negatives that never got around to making this key argument. You have to make an argument in the neg position explaining why privacy matters. There are any number of theories, but the most convincing one is that a sphere of privacy is key to freedom of thought, conscience and identity. If we are monitored constantly so that everyone can see what we do, say, and express at all times, there is no bubble of personal space within which to develop our honest character. If every aspect of our lives is subject to monitoring, we will engage in wholesale self-censorship in order to make sure that our actions meet with social approval. Put another way, our “self” -- that which makes us unique -- has to have a zone of privacy in order to develop authentically. Constant observation by others denies us the ability to develop an independent identity, and without that, no other values really matter.

Digital privacy is important to our relationships with other countries. This is true for two reasons. First, even though the resolution specifies that we’re talking about US citizens, it was widely reported in the wake of the Edward Snowden leaks that the US was also eavesdropping on people -- and leaders -- from *other* countries. This made many of our closest allies very angry, endangering vital diplomatic relationships. If we continue to violate digital privacy of our own citizens, they’ll probably assume that we’re still monitoring them, as well. Second, other countries look to the US (for better or worse) as a “bastion of liberty.” If we openly violate basic individual rights, then (A) we will lose global respect, and (B) rights will be endangered generally because we will lose the moral authority to insist on regimes of individual rights.

You might also note that digital privacy violations, empirically, will come to light. The Edward Snowden example shows this. No matter how secretive the government is, there will have to be private individuals, government workers or private contractors, who will operate the electronic snooping systems. Eventually, someone will leak or go to the press -- either because they think it’s morally right or because they want to go on the Tonight Show and be famous. So any benefits

of digital privacy violations are bound to be short-lived because there’s simply no way to develop

a reliably secret system.

National security as a concern is over-blown. We should resist the urge to respond to things because of “national security.” The 9/11 attacks were terrible, but overall, violence from terrorism is still vanishingly small in terms of its impact on society. The list of things that are more likely to kill you than terrorism is revealing and hilarious: lightning, your television, and (by far) the police! Our reaction to terrorism, and our willingness to subordinate our most fundamental rights to it, is profoundly irrational. That doesn’t mean that terrorist attacks can’t happen, but they are one among a wide variety of risks associated with daily life. And we blithely accept an array of activities that are vastly more dangerous than terrorism without so much as batting an eye -- driving a car, for instance, is far more deadly than terrorism, yet you don’t see people insisting that the government violate our basic rights in order to put an end to car-driving.

**AFFIRMATIVE EVIDENCE**

*DEFINITIONS*

## DIGITAL SURVEILLANCE DEFINITION

Nikki Gulzar et al, [Auckland University of Technology], "Surveillance Privacy Protection," [http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf,](http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf) 2013.

One of the cutting-edge surveillance technologies is digital surveillance. It involves the monitoring data and traffic on internet [64]. Government agencies such as Infor- mation Awareness Office, NSA and the FBI spend billions of dollars each year to develop systems so as to intercept and analyze the data transmitted, and extract the data that is useful to law enforcements [14].

*CIVIL LIBERTIES, PRIVACY, AND CONSTITUTIONAL RIGHTS*

## NSA SURVEILLANCE IS LEGAL

Bucci, Steven. [Dr., Director of The Heritage Foundation's Douglas & Sarah Allison Center for Foreign Policy Studies]. "Phone Records and the NSA: Legal and Keeping America Safe," Heritage Foundation. June 20, 2013, <http://blog.heritage.org/2013/06/20/phone-records-and-the-> nsa-legal-and-keeping-america-safe/

Over the past week, Snowden has inundated the world with details about the NSA collection of telephone records from companies such as Verizon. However, according to a FISA court order, Verizon was only ordered to hand over “metadata” of the calls it processed. Metadata refers to basic information, including telephone number, location, and duration of the call, and the court order does not authorize the government to access the content of such conversations. There is a growing body of legal precedent for the NSA program. In 1976 the Supreme Court upheld “the third party doctrine,” which states that anyone who voluntarily provides information to a third party, such as a telephone service provider, cannot object if it is later turned over to the government. What’s more, in 1979, the Supreme Court held in Smith v. Maryland that the government did not need a warrant to obtain phone record information as it did for the content of such communications. The information was not constitutionally protected because there was no true expectation of privacy. As a result, metadata collection is not protected under the 4th Amendment and is perfectly legal.

## SURVEILLANCE IS LEGAL AND DOESN'T VIOLATE PRIVACY

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The NSA's Phone Collection Order -

- It May be Legal, but is it Wise?," The Heritage Foundation. June 7, 2013,<http://www.heritage.org/research/commentary/2013/6/the-nsas-phone-collection-order-it-may-be-> legal-but-is-it-wise

First, some details. The order applies only to “meta-data” of calls: the phone numbers called, the location of the cell phone when the call was made, and the time and duration of the call. So the order does not require Verizon to let the NSA monitor the conversations or other content of the calls. Also, the order applies both to international calls and to calls occurring wholly within the United States. Verizon is required to update its compliance “on a daily basis.” Finally, though the order disclosed Wednesday applies only to Verizon, the logic of the request supports an inference that similar orders have been issued to other major telecommunications carriers like ATT & Sprint. In short, the order appears to give NSA blanket access to the records of Verizon customers' phone calls –foreign and domestic—made between April 25, when the order was signed, and July 19, when it expires. Of course, if the order is only the latest in a series of orders (as also seems likely), then the access may go back for quite some time. To a large degree this revelation it is not unexpected. We are a country still at war against Al Qaeda and its affiliates. As such, we need to have counterterrorism tools, such as Section 215 of the PATRIOT Act, which was apparently used in this case. And, though we don't yet know the details, it is important to note that since 9/11, the powerful tools have been modified and amended to maximize the protection of civil liberties to the extent possible. Here, the FISA court issued an order allowing for telephone calling data only, not the content of any calls. Such data are critical for link analysis -- connecting the dots between phone numbers in terrorist investigations. That is constitutional.

## LOSS OF PRIVACY IS INEVITABLE BUT SURVEILLANCE ENSURES BENEFITS FROM THIS LOSS

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012,<http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-> antique-privacy-rules

Ten years ago, surveying the technology of the time which, by and large, was one hundred times less powerful than today’s data processing capacity Scott McNealy, then-CEO of Sun Microsystems, said, “Privacy is dead. Get over it.”[14] He was, it seems, slightly wrong. Pure privacy—that is, the privacy of activities in your own home—remains reasonably well- protected.[15] What has been lost, and will become even more so increasingly, is the anonymity of being able to act in public (whether physically or in cyberspace) without anyone having the technological capacity to permanently record and retain data about your activity for later analysis. Today, large data collection and aggregation companies, such as Experian and Axicom, may hire retirees to harvest, by hand, public records from government databases.[16] Paper records are digitized and electronic records are downloaded. These data aggregation companies typically hold birth records, credit and conviction records, real estate transactions and liens, bridal registries, and even kennel club records. One company, Acxiom, estimates that it holds on average approximately 1,500 pieces of data on each adult American.[17] Since most, though not all, of these records are governmental in origin, the government has equivalent access to the data, and what they cannot create themselves they can likely buy or demand from the private sector. The day is now here when anyone with enough data and sufficient computing power can develop a detailed picture of any identifiable individual. That picture might tell your food preferences or your underwear size. It might tell something about your terrorist activity. Or your politics. This analytical capacity can have a powerful influence in law and policy and in particular in revealing links between the cyber personas and the real world activities of individuals. When we speak of the new form of “dataveillance,” we are not speaking of the comparatively simple matching algorithms that cross check when a person’s name is submitted for review when, for example, they apply for a job. Even that exercise is a challenge for any government, as the failure to list Abdulmutallab in advance of the 2009 Christmas bombing attempt demonstrates.[18] The process contains uncertainties of data accuracy and fidelity, analysis and registration, transmission and propagation, and review, correction, and revision. Yet, even with those complexities, the process uses relatively simple technologically—the implementation is what poses a challenge.

## NSA SURVEILLANCE ISN'T ANY WORSE FOR PRIVACY THAN HAVING A FACEBOOK ACCOUNT

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013,<http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

Granted there is something inherently creepy about Uncle Sam scooping up so much information about us. But Google, Facebook, Amazon, Twitter, Citibank and other companies know at least as much about us, because they use very similar data-mining programs to track our online movements. They gather that information in order to sell us products, and no one seems to be overly alarmed. The NSA is gathering that information to keep us safe from terrorist attackers. Yet somehow its actions have become a "scandal," to use a term now loosely being tossed around.

The real scandal here is that the Guardian and Washington Post are compromising our national security by telling our enemies about our intelligence-gathering capabilities. Their news stories reveal, for example, that only nine Internet companies share information with the NSA. This is a virtual invitation to terrorists to use other Internet outlets for searches, email, apps and all the rest. No intelligence effort can ever keep us 100% safe, but to stop or scale back the NSA's special intelligence efforts would amount to unilateral disarmament in a war against terrorism that is far from over.

## PRIVACY CONCERNS ARE NOT JUSTIFIED

Posner, Eric. [Law professor at the University of Chicago]. "I Don’t See a Problem Here," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-> surveillance-threat-real-or-imagined

The first objection strikes me as weak. We already give the government an enormous amount of information about our lives, and seem to have gotten used to the idea that an Internal Revenue Service knows our finances, or that an employee of a government hospital knows our medical history, or that social workers (if we are on welfare) know our relationships with family members, or that public school teachers know about our children’s abilities and personalities. The information vacuumed up by the N.S.A. was already available to faceless bureaucrats in phone and Internet companies — not government employees, but strangers just the same. Many people write as though we make some great sacrifice by disclosing private information to others, but it is in fact simply the way that we obtain services we want — whether the market services of doctors, insurance companies, Internet service providers, employers, therapists and the rest, or the nonmarket services of the government like welfare and security. Even so, I am exaggerating the nature of the intrusion. The chance that human beings in government will actually read our e- mails or check our phone records is infinitesimal (though I can understand that organizations like the A.C.L.U. that have a legitimate interest in communicating with potential government targets may be more vulnerable than the rest of us). Mostly all we are doing is making our information available to a computer algorithm, which is unlikely to laugh at our infirmities or gossip about our relationships.

## THE PROGRAM PREVENTS TERROR ATTACKS THAT PRESENT A BIGGER RISK TO FREEDOM

Nye, Joseph. [Professor of Government at Harvard University]. "Privacy gains the upper hand in the NSA surveillance debate," The Daily Star. August 19, 2013, <http://www.dailystar.com.lb/Opinion/Commentary/2013/Aug-19/227751-privacy-gains-the-upper-> hand-in-the-nsa-surveillance-debate.ashx#axzz2hEwSq0Dd

Rather than demonstrating hypocrisy and acceptance of the erosion of civil liberties, the Snowden disclosures have provoked a debate that suggests the U.S. is living up to its democratic principles in its traditionally untidy ways. America faces a trade-off between security and liberty, but the relationship is more complex than it appears at first glance. The worst threats to liberties come when insecurity is greatest, so modest trade-offs can sometimes prevent greater losses. Even such a great defender of freedom as Abraham Lincoln suspended habeas corpus under the extreme conditions of the American Civil War. And such decisions may not be recognized as mistaken or unjust until later – consider Franklin Roosevelt’s internment of Japanese-American citizens early in World War II. In the decade after Sept. 11, 2001, the pendulum of public sentiment swung too far to the security pole; but it has begun to swing back in the absence of major new terrorist attacks. A recent ABC News-Washington Post poll showed that 39 percent of Americans now say that protecting privacy is more important than investigating terrorist threats, up from only 18 percent in 2002. Ironically, the programs that Snowden revealed seem to have helped prevent massive new terrorism events, such as a bomb attack on the New York subways. If so, they may have prevented the implementation of more draconian anti-terrorist measures – thus enabling the current debate.

## CIVIL LIBERTIES ARE WELL PROTECTED

Gerecht, Reuel. [senior fellow at the Foundation for Defense of Democracies and a former case officer in the CIA’s clandestine service]. "The Costs and Benefits of the NSA," The Weekly Standard. June 24, 2013, <http://www.weeklystandard.com/articles/costs-and-benefits-> nsa\_735246.html

But journalists in Washington, who rub shoulders every day with national-security types, surely know that America isn’t that far gone. Civil liberties after 12 years of the global war on terrorism are actually as strongly protected in America as they were in 1999, when Bill Clinton was treating terrorism as crime and his minions were debating the morality of assassinating Osama bin Laden. The same is true in France and Great Britain, liberal democracies that have the finest, but also the most intrusive, counterterrorism forces in the West. Surveillance in these countries is intimate—the French internal-security service, the DST, and British domestic intelligence, MI5, bug and monitor their countrymen in ways that remain unthinkable in the United States. Yet the political elites and the societies of both countries have become much more sensitive to, and protective of, personal freedom as their internal security forces have grown more aggressive. It’s an odd and, for those attached to Friedrich Hayek’s Road to Serfdom, disconcerting

development: The massive American government, born of the welfare state and war, hasn’t yet gone down the slippery fascist slope. Liberal welfare imperatives may be bankrupting the country, but they have not produced a decline of most (noneconomic) civil liberties. Just the opposite.

American liberalism’s focus on individual privacy and choice has, so far, effectively checked the creed’s collectivism. America’s national-security state, which Greenwald believes has already become a leviathan, is, for the most part, rather pathetic.

*CYBERSECURITY*

## OUR CYBER INFRASTRUCTURE IS AT ENORMOUS RISK OF ATTACK—CURRENT JURISPRUDENCE IS INSUFFICIENT TO ENSURE SAFETY

Mark D. Young 11, [Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence], "Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security", Stanford Law & Policy Review 11 2011.

Linking hundreds of individual computer networks has created a virtual space on which much of the world's commerce and communication now¶ depends. Electronic mail, peer-to-peer data sharing, Voice-over-Internet Protocol (VolP), and wireless networks are examples of the technology that enables almost unlimited access to information. This access comes with significant risk. Criminals, terrorists, hostile nation-states, and foreign industrial competitors share this ubiquitous access to information. In the industrial age, we protected ourselves with high walls and long-range weapons; in the digital age, the availability and rapid development of cyber weapons requires layers of defenses and improved awareness of adversarial capabilities and intentions.¶ Since the first Internet transmission on October 29, 1969 we have been 2¶ deepening our dependence on digital communications. There are almost two billion users of the Internet. The United States economy depends on it; our critical infrastructure is controlled by it; and our national security is empowered by it, yet vulnerable because of it. Despite our digital dependence, our policy framework, our legal authorities, and our judicial precedent remain underdeveloped.¶ The cyber security legal landscape is a patchwork of federal and state statutes, federal regulation, and executive branch policy that evolved to address technologies that may no longer exist. Federal government "capabilities and responsibilities are misaligned within the U.S. government.' There is no shortage of threats to our information infrastructure. The media has reported that computer-controlled electric power grids are "plagued with security holes that could allow intruders to redirect power delivery and steal data . . . ."5 Other reports claim that the Chinese military is responsible for the highly sophisticated January 2010 attack against Google's corporate network that sought to access the company's source code.6 According to the Congressional Research Service, "[t]hreats to the U.S. cyber and telecommunications infrastructure are constantly increasing and evolving as are the entities that show interest in using a cyber-based capability to harm the nation's security interests."¶ This Article will review the history of electronic surveillance authorities, explain how these authorities are relevant to today's cyber security issues, identify the insufficiencies of the three specific laws on this topic, and recommend discrete amendments to these statutes. The text highlights the deficiencies in the authorities governing U.S. government action in cyberspace and argues that specific sections must be amended to enhance cyber security and enable information sharing between the public and private sector. This Article does not address the federal statutes that govern cybercrime. It focuses on cyber security authorities in the national security context, but the legislative changes recommended here will also benefit law enforcement operations.

## CURRENT LEGAL INSUFFICIENCIES HAMSTRING OUR CAPABILITIES TO PREVENT TERRORISM AND ENSURE CYBERSECURITY—LEGAL ACTION IS NECESSARY

Mark D. Young 11, [Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence], "Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security", Stanford Law & Policy Review 11 2011.

he electronic surveillance authorities discussed above are relevant to national security investigations because computer servers and ISPs are provided privacy protections under U.S. law and there is an expanding possibility that terrorists will hold dual citizenship. An example of the unique circumstances under which federal law enforcement and the American intelligence community must now operate is the status of Anwar al-Awlaki. This radical Muslim cleric was born in New Mexico in 1971. As an illustration of the significance of the dual citizenship issue, there has been recent debate about the Obama administration's authorization for the targeting and killing of al-Awlaki.s?¶ These statutes are also relevant to U.S. cyber activities because of the definition of electronic surveillance:¶ The acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under¶ circumstances in which a person has a reasonable expectation of privacy and a 58¶ warrant would be required for law enforcement purposes.¶ The definition also includes the collection of communications content if it¶ occurs within the United States.5 9 Thus, if the government wanted to see the content of an e- mail sent from al-Awlaki to a recipient in Saudi Arabia, but collected the e-mail from somewhere within the United States, the collection is electronic surveillance and subject to the limitations of electronic surveillance law. The definition means that national security and law enforcement investigations, which include online monitoring, are subject to the Fourth Amendment and the regulations that have evolved with electronic surveillance authorities.¶ The final parts of the electronic surveillance definition accommodate the¶ decision in Katz incorporating the acquisition of the contents of any communication "in which a person has a reasonable expectation of privacy¶ and a warrantwould be requiredfor law enforcementpurposes,and if both the sender and all intended recipients are located within the United States." 60¶ According to a National Defense University International Cyber Security Conference:¶ The first requirement when seeking to coalesce cyberspace governance is the recognition that spoken and written words form the foundation of our understanding of cyberspace and its governance. As such we need to come up with clear definitions if effective governance is to exist. We also need a common lexicon and broader understanding of criminal threats, governance tools and what constitutes cyber security.61¶ The cyber lexicon remains confusing. The Department of Defense's Dictionary of Military and Associated Terms originally defined cyberspace as "the notional environment in which digitized information is communicated¶ over computer networks."62 The definition was amended in 2008 to a "global¶ domain within the information environment consisting of the interdependent¶ network of information technology infrastructures, including the Internet,¶ telecommunications networks, computer systems, and embedded processors¶ 63 and controllers."¶ A new definition of cyber space has been published by the Vice Chairman of the Joint Chiefs of Staff: "[A] [d]omain characterized by the use of electrons and the electromagnetic spectrum to store, modify, and exchange data via¶ 64¶ network[ed] systems and associated physical infrastructures." There are¶ myriad definitions of cyberspace-and associated terms-that confuse the¶ 65 issues within the federal government.¶ According to a cyber security workshop hosted by the American Bar Association's Standing Committee on National Security, the National Strategy Forum, and the McCormick Foundation, "the laws of intelligence collection have applicability to our cyber activities in two contexts: as rules of authorization and limitation within the domestic sphere and as rules of public disclosure."66 The workshop report acknowledges the intelligence community's concerns about cyber vulnerabilities that may enable adversarial cyber intrusions. The intelligence community may share cyber vulnerability information within the U.S. government, but current law prohibits the government from disclosing the same information to the private sector. In the cyber domain-most of which is owned by the private sector-information sharing between the government and private sector is largely prohibited. "This is one legal area

that clearly requires work."6 7¶ The definitions of cyber space are illustrative of the different understandings held by different parts of the government. It is difficult to discuss the privacy, policy, and legal issues surrounding the national security sector's cyber activities if no one agrees on what cyber space is. The inconsistent understanding compounds the challenge of discussing how electronic surveillance should be regulated. Cyber investigations are a significant instrument for monitoring terrorist and adversarial state activity, but without at least a general understanding of cyber space and how much government activity is appropriate in cyber space, we are less secure and may be providing criminals and terrorist an online sanctuary. A. Legal Insufficiencies¶ The government is attempting to protect national interests from myriad cyberspace threats and shift its organizational structures to better manage its limited cyberspace resources. It is doing this, however, without adjusting one of the biggest cyber vulnerabilities facing the country: insufficient legal authorities to allow federal action in the cyber domain. According to the Quadrennial Defense Review (QDR) Independent Panel, established by Congress "to review the QDR, assess the long term threats facing America, and produce recommendations regarding the capabilities which will be necessary to meet those threats,"68 national security planners must use a comprehensive approach to address current threats. The panel recommended a review and restructure of the laws governing the armed forces and national defense. To better address cyber threats aligning against U.S. interests, criminal statutes must be included in any analysis that seeks to improve interagency coordination and clarification of departmental and agency authorities and¶ responsibilities.¶ The first and most significant cyber policy issue in the national security¶ arena concerns covert action. There is ongoing debate among government lawyers about the Pentagon's legal authority to disrupt a foreign network during peacetime operations. "The CIA has argued that doing so constitutes a 'covert' action that only it has the authority to carry out, and only with a presidential order."69 Others argue that the Defense Department can conduct¶ traditional military activities online. 70¶ The extant legal authorities governing cyber activities within the¶ Department of Defense provide insufficient statutory authority for military cyber operations. According to General Keith Alexander, the Commander of U.S. Cyber Command and the Director of the National Security Agency, "offensive [cyber] capabilities must be based on 'the rule of law.' 71¶ The Department of Defense believes its current authority provides significant intelligence authority to the Secretary of Defense. Title 10 is vague about the intelligence responsibilities of the Secretary of Defense.72 Title 50 acknowledges that the Defense Department conducts intelligence operations in support of military operations. It also mandates that the Secretary of Defense ensure that "the tactical intelligence activities of the Department of Defense complement and are compatible with the intelligence activities under the National Intelligence Program." 73 The lack of clarity in the authorities of the Department of Defense exacerbates the challenges of cyber operations. If it is unclear whether the clandestine collection of information from a foreign computer network is "defense-related intelligence," then it will be unclear whether it is within the Defense Department's authority to collect that information. It also remains to be decided if computer network operations should be classified as covert action.¶ Covert action is "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or¶ acknowledged publicly."74 It does not include "activities the primary purpose of which is to acquire intelligence" or "traditional diplomatic or military activities or routine support to such activities."75 The term traditional military activity is not defined by statute or military doctrine. The inherent anonymity of actions in cyberspace does not mean the operation is a covert action, merely because the Defense Department fails to acknowledge its involvement publicly. As a policy matter, we must decide into which category the online activities of our military and intelligence agencies belong. Without this policy decision, our ability to use cyberspace to protect American interests is significantly burdened. We must decide if everything each of the elements of our national security community does on computer networks is subject to electronic surveillance law.¶ Second, we must reconsider our concept of online privacy. Within a relatively short period of time, there have been significant shifts in what different age groups consider private.¶ Younger "Digital Natives" have a culture of sharing built though forwarded e-mails and social-networking site posts. Their idea of privacy is different from older "digital immigrants." Digital natives have:¶ [O]ver 10,000 hours playing videogames, over 200,000 emails and instant messages sent and received; over 10,000 hours talking on digital cell phones;

over 20,000 hours watching TV (a high percentage fast speed MTV), over 500,000 commercials seen-all before the kids leave college. And, maybe, at the very most, 5,000 hours of book reading. Cyber security presents novel issues that cut across areas of law that have successfully represented our national values, but now may not be appropriate for current technology. We may have to review how much Fourth Amendment protection we provide to online activity. The legal regimes governing electronic surveillance have unsuccessfully tried to remain current with modern technology. The Supreme Court's opinion in Katz v. United States notwithstanding, some argue that the Fourth Amendment should not protect some forms of online communications.

Professor Orin Kerr argues that the "contents of online communications ordinarily should receive Fourth Amendment protection but that non-content communications should not be protected." "Online, non-content surveillance is usually surveillance related to identity, location, and time; content surveillance is surveillance of private¶ thoughts and speech."¶ The distinction between government surveillance of activities within¶ enclosed spaces and government surveillance in public space is applicable to government surveillance online. "So long as conduct is out in the open, it is not protected by the Fourth Amendment." 79 In contrast, "entering enclosed spaces ordinarily constitutes a search that triggers the Fourth Amendment."80 The inside/outside distinction in the physical domain should be applied as a content/non-content distinction in the cyber domain.¶ Internet surveillance of non-content information should not trigger the Fourth Amendment just like surveillance of public spaces does not trigger the Fourth Amendment.

Surveillance of content should presumptively trigger the Fourth Amendment in the Internet setting just like surveillance of inside spaces¶ presumptively triggers the Fourth Amendment in the physical world.8 1¶ Kerr does acknowledge that the difference between content and non- content information can be difficult to determine.82 Adopting the content/non- content distinction, however, would be useful in evolving electronic surveillance laws that are critical to ensure the national security community has both adequate legal authorities with which to apply its evolving cyber capabilities. It would put the military and intelligence agencies on firmer¶ foundations to conduct cyberspace activities.¶ Some critics of the content/non-content paradigm argue that Internet¶ surveillance is less-expensive, easier to conduct, and much more invasive than¶ conventional surveillance. While this may be true in some circumstances, "online surveillance varies greatly in its ease, cost, and invasiveness: it can be cheap, easy and highly invasive, or it can be expensive, difficult, and much less invasive than physical surveillance."a The expanding use of commercially available encryption, anonymizers, and proxy servers makes Internet surveillance much more difficult, expensive, and time consuming.

*AMEND ECPA*

## AMENDING THE ECPA IS KEY TO FACILITATING COOPERATION BETWEEN ISPS AND THE GOVERNMENT, WHICH IMPROVES NATIONAL SECURITY

Mark D. Young 11, [Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence], "Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security", Stanford Law & Policy Review 11 2011.

The National Security Strategy prioritizes the prevention of nuclear weapons proliferation to violent extremists. Counterterrorism operations have been an obvious priority since September 11, 2001. The United States has a clear interest in deterring terrorism; in order to do that, the national security elements of the federal govemment must have adequate authority to investigate terrorists and act once they are discovered.¶ Modem technologies provide a means of coordination for terrorists, just as¶ they make communication and commerce more convenient.

The technology¶ provides anonymity, convenience, and rapid communication. E-mail, peer-to-¶ peer connections, voice over intemet protocol (VoIP), and social networks such¶ as Facebook and MySpace provide forums for extremists to share their¶ ideologies and their techniques and procedures for conducting illicit activities.¶ 88¶ With the enactment of the ECPA, Congress sought to adapt privacy¶ protections to technologies that were new in 1986.89 The statute was effective in protecting communications privacy until technology and network structures developed in such a way as to hinder reasonable law enforcement and national security investigations.

Modem technology has made ECPA "unwieldy and unreliable . . . immensely difficult for judges and investigators to apply, confusing, costly, and full of legal uncertainty for communications and other technology tools and service providers, and an unpredictable guardian of our country's long cherished privacy values." 90 The confusion with ECPA also has an impact on national security investigations. Under ECPA, government access to an e-mail from a potential terrorist is subject to different legal standards depending on when the recipient accessed the e-mail. 91 If the e-mail is stored and has not yet been accessed by its recipient, ECPA requires a warrant for the government to see its contents.92 Once the same e-mail is opened, the government may access the content with a subpoena.93 Although there is disagreement among circuit courts on this "open and unopened" communications distinction, according to the Department of Justice, the government may subpoena the e-mail contents if they are more than 180 days old.94 "The different standards are the unanticipated byproduct of technology changes, and not a careful balancing of the needs of law enforcement and the privacy rights of individuals." 95 Issuance of a wiretap warrant requires probable cause, but ECPA requirements "prohibit[] law enforcement from using wiretaps in the early stages of an investigation and make it one of the hardest warrants to obtain." The needs of the national security community are similarly impacted by these ambiguous standards.¶ The ECPA applies to all online communications. It includes VolP communications.97 The "by the aid of wire, cable, or other like connection" requirement includes wireless connections such as mobile phones, satellites, and fiber-optic cables. 98 The law also protects communications that are "furnished or operated by any person engaged in providing or operating such facilities" for communications. 99 In the computer context, "software installed on two computers may be the 'facility' for communication."'oo¶ Any federal law enforcement or intelligence activity online will implicate ECPA. However, sections of ECPA are clearly inconsistent with U.S. national security. Most agree that federal cyber security efforts must include better partnering between the federal and private sectors.101 According to Melissa Hathaway, former Acting Senior Director for Cyberspace at the National Security Council, "the ISPs want to provide threat data, but the government either can't take it or won't."l02 Lawyers for the major data providers interpret the ECPA to prohibit the voluntary provision of customer data. In some cases, "the government won't take the [threat] information because they have no technical way to receive it."103 Hathaway explained that various providers format their information differently and that the national security sector cannot receive, store, or analyze the large volumes of information even if the ISPs did make it available to the government.¶ It is understandable why the private sector is concerned about breaking this law. Criminal violations of

ECPA may make an offender liable for fines or up to five years in prison, or both.104 Civil liability includes injunctive or declaratory relief, and damages of at least $10,000.05¶ Under § 2702 of ECPA, civil liability attaches for the unlawful disclosure of communications data by service providers.106 Notwithstanding the extensive list of exceptions and defenses to this liability,'o7 service providers are less willing to provide data to the government after the controversy and legal suits that followed the December 2005 disclosure of the Terrorist Surveillance Program at the National Security Agency.o Litigation against the service providers for allegedly unlawfully providing customer data to the government continues today. 109 The legal issue with the TSP arose "because the data NSA tapped reportedly came in by fiber-optic cable, so FISA applied unless the physical tap took place outside the sovereign territory of the United States - a few miles offshore for example.""l0¶ The statute prohibits wiretapping and electronic surveillance in certain circumstances. "An interception can only be a violation of ECPA if the conversation or other form of communication intercepted is among those kinds which the statute protects, in oversimplified terms - telephone (wire), face-to- face (oral), and computer (electronic)."' 1 1 "Surreptitious 'access' is at least as great a threat as surreptitious 'interception' to the patrons of electronic mail (e- mail), electronic bulletin boards, voice mail, pagers, and remote computer storage."' 12¶ These sections that limit the interception of, access to, and disclosure of data in transmission require amendments in order to better protect the privacy of American citizens while allowing the national security community to remain current with the online activities of adversaries. Amendments to § 2702 allowing more flexibility for the ISPs would reduce their reluctance to share threat data with the government. As previously noted, "while a failure to follow the ECPA in obtaining e-mail information may not result in suppression of the evidence, it may result in civil liability for ECPA violators."" 3¶ The Department of Justice's Office of Legal Counsel has opined that an ISP may not even disclose its relationship with a customer without a national security letter.l14 According to this opinion, "when the FBI identifies a subscriber by name, section 2702(a)(3) [of the ECPA] forbids a provider from divulging the existence of that person's or entity's subscription with the provider.""l5 ECPA also prohibits ISPs from identifying a customer if the FBI provides a phone number instead of a name. Without consent from a customer, ECPA prohibits the voluntary provision of information by the ISPs. In some cases, it even limits what can be provided by the ISPs with a national security¶ letter.¶ Section 2709(b)(1) limits what the FBI can request and what an ISP may¶ provide under a national security letter to the name, address, length of service, and local and long distance toll billing records of a person or entity." 6 The structure of the statute also supports these limitations on the sharing of subscriber information: "Section 2709 is an exception to the background rule of privacy established by 18 U.S.C. § 2702(a), which bars a provider from giving the Government a record or other information pertaining to a subscriber or customer."" 7 Private defendant suits are still being litigated against telecommunications companies after the disclosure of the TSP.118 Despite the outcome of past and pending TSP litigation, private sector companies are less likely to assist the government in law enforcement or national security investigations if their cooperation risks a civil suit.¶ Any amendments permitting a less burdensome regime for government access to information, for which the public believes it has an expectation of privacy, may cause civil liberties concerns, but these may be mitigated through a statutory definition of the types of data the ISPs could share and the setting of guidelines under which the data could be shared. For example, the Communications Assistance for Law Enforcement Act (CALEA) was created to ensure that telecommunications companies had the capabilities "to assist law enforcement in conducting digital electronic surveillance regardless of the specific telecommunications systems or services deployed."' 19¶ A similar approach should be used to allow the ISPs to share either metadata or content data with the government. An amended ECPA could include a provision that allows the disclosure of customer information, describing imminent acts dangerous to human life that are violations of the criminal laws of the United States, and not protected by the First Amendment to the U.S. Constitution. If the information describes imminent activity to "intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; [or] to affect the conduct of a government by mass destruction, assassination or kidnapping" ISPs should not be held liable for disclosing this information without a court order.120 Such an amendment could outline the process by which the government should work with the ISPs to enhance their ability to detect threats to national security.

*AMEND SCPA*

## TITLE II OF THE ECPA (THE SCA) SHOULD BE AMENDED TO ALLOW THE NATIONAL SECURITY COMMUNITY TO ACCESS THREAT INFORMATION.

Mark D. Young 11, [Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence], "Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security", Stanford Law & Policy Review 11 2011. RFK

Title II of the ECPA regulates access to stored communications and records.'2' It distinguishes between data in transit and data at rest. These distinctions are artificial, however, in light of the development of technology such as cloud computing' 22 and remote computing services. "Today, the distinctions between and among data in transit, data in electronic storage, data stored by a remote computing service, and data more [than] 180 days old no longer conform to the reasonable expectations of Americans, nor do these distinctions serve the public interest." 23 These distinctions are irrelevant in the context of national security operations. "The SCA prohibits the unauthorized access to an electronic communication service or facility 'and thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communications while it is in electronic storage."' 1 24 Thus, "when a¶ communication is in transmission between the source and the destination, the¶ ,,125¶ ECPA governs. However, when a communication reaches its destination,¶ the SCA governs.126¶ Arguing against an "automobile-exception"1 27 to the Fourth Amendment warrant requirement for computer information, Orin Kerr argues that "computer data moves in a very different sense than automobiles or ships move."l28 In contrast to what occurs when law enforcement officers lose track of a vehicle in the process of getting a warrant, computer data is copied, rather than being physically moved. "When a file is transferred from one place to another, a new copy is generated and that new copy is sent to the new place. The old copy is ordinarily left behind. Further, when a copy is made, that copy can be controlled and protected from interference." Kerr concludes that, since the data remains on a computer, the government "can copy the data-or order a copy to be made by the server that hosts the data-and then access the copy at a later time."l29 Because the data is not destroyed and is still accessible, "there is no general exigency that justifies a rule that the government can access Internet communications without a warrant." 30¶ However, Professor Kerr underestimates the operational security practices¶ of terrorists and criminals. Commercially available encryption, proxy-servers, unknown e-mail accounts, and small, highly concealable storage media negate Kerr's argument. Data can disappear, or be made inaccessible in seconds. Computer hard drives can be destroyed in five seconds,' ' and small storage media can hold eight gigabits of data on a device no larger than a quarter.132 Because data can quickly be made inaccessible, there should be an exigency exception for the warrant requirement for computer data. In the national security context, warrants are inappropriate in cases where a U.S. citizen is not the target of the investigation. If the investigation does involve an entity protected by the Fourth Amendment, then there should be a legal accommodation to access fleeting data without an aprioriwarrant application.¶ The distinction between stored and transit data may not be as relevant today as it was when the SCA was passed, but the statute also distinguished between electronic communications service providers and remote computing service providers.1 33 Each is subject to distinct exceptions for consent disclosures. Communications content may be disclosed with consent from only one party to the communication. In contrast, remote computing service providers . . . may also disclose with the consent of a subscriber to the service.134 In 2008, the Ninth Circuit held that the provider of a text messaging service was an electronic communications service provider rather than a remote computing service provider, and consequently, it was in violation of the Section 2702 when it disclosed to the city-subscriber the content of messages sent to and from a city employee's pager.135¶ There is little judicial consensus concerning how SCA should be applied to contemporary communications. The difficulty flows from the fact that the definitions used for terms in section 2703 were crafted for the technology of an earlier day. Application becomes an issue because under one construction the content of electronic communications can only be

secured under a warrant; under another, a subpoena will suffice; and under a third, the required disclosure provisions of section 2703 do not apply at all. A warrant is required for disclosure to authorities by a provider of "electronic storage" of the contents of a communication "in electronic storage" in a wire or "electronic communications system" for less than 181 days.13 A subpoena or court order will suffice after 180 days or when authorities seek content disclosure from a provider of "remote computing service" of a communication "held or maintained on that service -

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission), a subscriber or customer of such remote computing service; and (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." 137¶ One court has concluded that a web-based e-mail provider must comply with a criminal trial subpoena for the contents of a subscriber's opened e-mail¶ 138¶ The district court determined that the e-mail was not in the type of "electronic storage" that would have triggered the application of section 2703(a)'s warrant¶ requirement. The court reasoned that the e-mail of web-based users is not in electronic storage because it does not fit the "backup" requirements of 2510(17)(B). From the court's perspective, the backup reflects the practice of non web-based e-mail users who download their e-mail to their own computers and only leave their e-mail with their service provider as backup. Web-based e- mail users may store their e-mail with their providers, but since they ordinarily do not download them such storage cannot be considered backup.139¶ The SCA makes it more difficult for the federal government to access Facebook and MySpace communications. Private litigants were unsuccessful when they sought to acquire webmail and private messaging from Facebook¶ and MySpace in Crispinv. ChristianAudigier, Inc.140 The litigants argued that the subscribers whose communications were at issue had no standing.141 Nor could they convince the court that section 2703(e), which immunizes providers from compliance with court orders and subpoenas, contemplated private party access to provider-held customer communications.¶ Federal officials may secure electronic communications service or remote¶ computing service customer-related transaction information (name, address, means of payment, etc.) under an administrative subpoena without the necessity of notifying the customer. 143 If an ISP is served a search warrant for electronic communications content, pursuant to 18 U.S.C. § 2703(a) the service provider must comply with Rule 41 of the Federal Rules of Criminal Procedure, which includes providing a copy of the warrant and receipt for any property seized to the service provider as required by Rule 41(f)(1)(C).144 Neither SCA nor the Fourth Amendment, however, requires them to notify the¶ person to whose communication they have access.145¶ Like the ECPA, the SCA should contain additional provisions that permit¶ more information sharing between the private sector and the government in context of national security. The need for severe sanctions for abusing this information sharing should be balanced as to not chill the relationship between the government and private sector in the information sharing arena. "Lack of statutory clarity [may cause] judicial uncertainty,"1 46 but it may also prevent the national security community from accessing threat information that could interrupt an attack against Americans or American interests. Because courts are increasingly denying government requests for retrospective geolocation data without a warrant (citing the SCA), 147 statutory amendments must include the authority for the national security community to access this information.

*AMEND FISA*

## FISA SHOULD BE AMENDED

Mark D. Young 11, [Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence], "Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security", Stanford Law & Policy Review 11 2011.

The Foreign Intelligence Surveillance Act of 1978 established a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes." 49 Amended many times since passage, FISA governs most national security electronic surveillance. Its threshold requirement is "probable cause to believe that 'the target of the¶ electronic surveillance is a foreign power or agent of a foreign power."' Even in its amended form, FISA hinders national security investigations. 150¶ FISA has been outpaced by technology.

According to Benjamin Wittes, "the communications and data infrastructure FISA sought to regulate no longer exists . . . . Current cyber security threats require access to data from cyberspace with appropriate executive, legislative, and judicial oversight mechanisms. Electronic surveillance law must recognize that in the world of social networking, instant messages, and packetized data streams, state boundaries are meaningless. Rather than being geographically focused, surveillance law needs to be at least as concerned with how data is used as it is about "how easily [the] government can collect it in the first place."' 5 2¶ FISA's standards for access by the government to electronic communications are much more demanding than those under the SCA.s 3 The few publicly available FISA decisions indicate that litigation may arise under sections 1806(f) and 1825(g) that allow for limited challenges to the exercise of FISA authority in the context of electronic surveillance and physical searches.154 After the Terrorist Surveillance Program was disclosed in 2006, the Electronic Frontier Foundation sued AT&T for assisting NSA with the surveillance of AT&T customers. 55 There was strong debate in the U.S. Senate about new FISA legislation that granted "retroactive immunity to telecommunications companies that assisted the NSA in warrantless surveillance of Americans."l 5 6 Some senators argued that "telecommunications companies should not be punished for assisting the government in its fight against terrorism." 57 Others argued that the bill rewarded telecommunications companies for violating the law and betraying the privacy of their customers. Despite dissent, the bill passed and President Bush signed the FISA Amendments Act of 2008 into law on July 10, 2008."5s¶ The FISA, even in its amended form, has already hindered counterterrorism network surveillance.159 An important addition to FISA under this Act was its expansion of FISA's coverage to include surveillance of Americans living overseas. Under § 702(b) of FISA, the government may not "intentionally target a United States person reasonably believed to be located outside the United States." 60 Previously there was no procedure for obtaining a warrant for surveillance of Americans overseas because magistrate judges had no extraterritorial jurisdiction under the Federal Rules of Criminal Procedure.161 "By placing Americans overseas under FISA, Congress created a procedure for protecting the privacy of all Americans subject to foreign intelligence surveillance."l62 In addition, Section 702 outlines the procedures for targeting non-U.S. citizens outside the United States.'63 It includes a provision that prohibits the intentional electronic surveillance of "any person known at the time of acquisition to be located in the United States."'a This means that the collection of a terrorist target must stop when and if the government discovers that the target of surveillance has landed in the United States.¶ Section 703 outlines the Foreign Intelligence Surveillance Court's authority for approving the surveillance of U.S. persons outside the United¶ States.' 6 5 It states:¶ The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored¶ electronic data that requires an order under this Act, and such acquisition is conducted within the United States.¶ If a UnitedStatespersontargetedunderthissubsectionis reasonablybelieved to be located in the United States during the effective period of an order issuedpursuant to subsection (c), an acquisition

targetingsuch United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States while an order issued pursuant to subsection (c) is in effect. Nothing in this section shall be construed to limit the authority of the Government to seek an order or¶ authorization under, or otherwise engage in any activity that is authorized¶ 166 under, any other title of this Act.¶ This section emphasizes that electronic surveillance must stop when the government recognized that the target is inside the United States. Until recently, these protections seemed reasonable in accordance with the Fourth Amendment and to have little effect on the electronic surveillance of terrorist targets. The growing number of U.S. citizens or dual citizenship terrorists has changed this calculus. With U.S. persons now recognized as potential terrorists, electronic surveillance laws such as the FISA must adapt to allow the access of computer network communications such as e-mails and instant messages to be collected. Under the current regime, electronic surveillance of any target must stop once the government recognizes the target is in the United States. Furthermore, if the target is recognized as a U.S. citizen that collection must stop until the intelligence community obtains approval from the Foreign Intelligence Surveillance Court.¶ The FISA must be adjusted to accommodate for the

U.S. citizen terrorist and to close the gap between section 702 and FISA Title I collection. There must be amended FISA language that accommodates the transfer of collection from authorities found under section 702 and those under FISA Title I. In 2000, future Director of National Intelligence Mike McConnell said that "New thinking is required ... to harness [signals intelligence] capabilities to control vulnerabilities of the information age."' 67 McConnell was prescient in describing the challenges now shared between the National Security Agency and U.S. Cyber Command:¶ No other government agency, now or in the foreseeable future, will match NSA's ability to detect and react to an information attack. This point is controversial because today cyber penetrations are no longer hindered by traditional borders, and it is increasingly difficult to distinguish between foreign and domestic threats; yet, NSA's capabilities are limited to use against only foreign targets. Now that telecommunications and networking have eliminated many of the traditional boundaries that protected the United States from foreign influence and activity, we need to think differently about how to¶ 168 use and develop NSA's capabilities.¶ The FISA is an important capability used by the national security community. Malicious activity in cyberspace is difficult to classify as a "foreign nation state [attack] - an intelligence and defense or national security event, a domestic attack - a law enforcement concern - or an attack by a terrorist group - a law enforcement concern as well as an intelligence and defense or national security event."1 6 9 Modem electronic surveillance authorities must incorporate this reality and enable the power of the national security community to be applied in a manner that is effective and effectively overseen.

*BINARY SEARCHES*

## BINARY SEARCHES CAN LIMIT THE VIOLATIONS OF PRIVACY.

Ric Simmons, [Professor of Law, Ohio State University], "Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment," Harvard Journal of Law & Public Policy, 2012.

Binary surveillance refers to a surveillance method that only ¶ produces one of two results: positive (meaning that illegal ac-­‐¶ tivity has been detected) or negative (meaning that illegal activ-­‐

¶ ity has not been detected).92 The surveillance provides no other ¶ information about the person or area being monitored, and so ¶ represents a relatively minor intrusion on the target’s privacy. ¶ In fact, the Supreme Court has held that binary surveillance ¶ does not even count as a “search”

under the Fourth Amend-­‐¶ ment because it does not infringe on an expectation of privacy ¶ that

society is prepared to recognize as legitimate.93 ¶ A simple example of a binary surveillance technique is a field ¶ test for narcotics. If a law enforcement officer reasonably be-­‐¶ lieves that a certain substance may be narcotics, she can legally ¶ seize a very small amount of the substance

and mix it with cer-­‐¶ tain chemicals.94 If the substance tests positive for narcotics, the ¶ law

enforcement officer knows that the substance is in fact con traband and that a crime has occurred. If the substance tests ¶ negative, the officer knows nothing about the substance other ¶ than the fact that it is not an illegal drug. Therefore, because the ¶ suspect has no legitimate interest in possessing contraband, ¶ assuming other procedural prerequisites are satisfied, the

sur-­‐¶ veillance does not implicate the Fourth Amendment95—the of-­‐¶ ficer either learns nothing

at all about the defendant or learns ¶ that the defendant is engaging in illegal activity.

**SURVEILLANCE DOESN'T UNDERMINE DEMOCRACY - IT HELPS ACTUALLY HELPS IT**

Posner, Eric. [Law professor at the University of Chicago]. "The Secrecy Paradox," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-> threat-real-or-imagined

This brings me to another valuable point you made, which is that when people believe that the government exercises surveillance, they become reluctant to exercise democratic freedoms. This is a textbook objection to surveillance, I agree, but it also is another objection that I would place under “theoretical” rather than real. Is there any evidence that over the last 12 years, during the flowering of the so-called surveillance state, Americans have become less politically active? More worried about government suppression of dissent? Less willing to listen to opposing voices? All the evidence points in the opposite direction. Views from the extreme ends of the political spectrum are far more accessible today than they were in the past. It is infinitely easier to get the Al Qaeda perspective today — one just does a Google search — than it was to learn the Soviet perspective 40 years ago, which would have required one to travel to one of the very small number of communist bookstores around the country. It is hard to think of another period so full of robust political debate since the late 1960s — another era of government surveillance.

*GOVERNMENT SECRECY*

## SECRET GOVERNMENT PROGRAMS ARE NECESSARY AND EFFECTIVE

Posner, Eric. [Law professor at the University of Chicago]. "The Secrecy Paradox," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-> threat-real-or-imagined

The question raises a real paradox. If government can keep secrets, then the public cannot hold it to account for its actions. But if government cannot keep secrets, then many programs — including highly desirable ones — are impossible. Many commentators seem to think that the answer is to keep secrecy to an absolute minimum, but this response is far too easy. One reason it is too easy is that it implies that secrecy can be exceptional. Government secrecy in fact is ubiquitous in a range of uncontroversial settings. To do its job and protect the public, the government must promise secrecy to a vast range of people — taxpayers, inventors, whistle- blowers, informers, hospital patients, foreign diplomats, entrepreneurs, contractors, data suppliers and many others. But that means that the basis of government action, which relies on information from these people, must be kept secret from the public. Economic policy is thought to be open, but we saw during the financial crisis that government officials needed to deceive the public about the health of the financial system to prevent self-fulfilling runs on banks. Then there are countless programs that are not secret but that are too complicated and numerous for the public to pay attention to — from E.P.A. regulation to quantitative easing. N.S.A. surveillance blends into this incessant, largely invisible background buzz of government activity; there is nothing exceptional about it.

## EXPERTS WITH ACCESS TO SECRET INFORMATION PROVE IT WORKS

Foust, Joshua. [Fellow at the American Security Project]. "These Programs Exist Because They Work," The New York Times. June 10, 2013,<http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-> imagined

The government, too, faces a Catch-22 in defending itself: discussing the success of these programs would, by design, require removing secrecy about them. If they only work because they’re secret, then that’s a tough choice to make. At a political level, too, the effectiveness argument is vitally important. Director of National Intelligence James Clapper has called the leaks “literally gut-wrenching,” not because he is an evil man who loves violating privacy laws but because he seems to genuinely believe those exposed programs work. The Senate Intelligence Committee chairwoman, Diane Feinstein, too, has claimed that the N.S.A. effectively disrupts terror attacks. Last week’s exposure of the N.S.A.’s surveillance programs does not address whether they were effective or not. But they exist because the people who created and oversee it believe they are effective. If we’re to end those programs, we should grapple with the possibility that we’re also losing the means to prevent future attacks.

## NSA PROGRAMS ARE LEGAL BUT INTERNAL SECURITY WAS TOO LAX.

PressTV, "NSA Chief Defends Surveillance Programs," [http://www.presstv.ir/detail/2014/05/13/362422/nsa-chief-defends-surveillance-programs/,](http://www.presstv.ir/detail/2014/05/13/362422/nsa-chief-defends-surveillance-programs/) May 13, 2014.

In his first interview since taking the helm of both the NSA and US Cyber Command in April, Mike Rogers said the programs were legal and needed better explanation rather than an overhaul.¶ Last year, former NSA contractor Edward Snowden leaked details of numerous top-secret NSA surveillance programs to media. The revelations damaged US ties with allies like Germany and France by showing the level of Washington’s spying activities on them over years.¶ Rogers told the Reuters Cybersecurity Summit in Washington that some NSA staff were "confused" by the onslaught of criticism because a series of official reviews found that the agency had for the most part abided by US law.¶ He said the agency’s internal security, which allowed Snowden to remove thousands of secret documents, had been too lax. "Clearly we should not have allowed this to happen," Rogers said.

## SURVEILLANCE IS NECESSARY TO PROTECT NATIONAL SECURITY.

Alan Dershowitz, [Harvard University], Debate with Michael Hayden, Alexis Ohanian, and Glenn Greenwald, Toronto, transcript available at The Atlantic, <http://www.theatlantic.com/politics/archive/2014/05/false-equivalence-on-surveillance-from-alan-> dershowitz/361694/, May 5, 2014.

Our enemies, especially those who target civilians, have one major advantage over us. They are not constrained by morality or legality. We have an advantage over them. In addition to operating under the rule of law, we have developed through hard work and extensive research technological tools that allow us to monitor and prevent their unlawful and lethal actions. ¶ Such technological tools helped us break the German and the Japanese code during the Second World War. They helped us defeat fascism. They helped us in the Cold War. And they are helping us now in the hot war against terrorists who would bomb this theater if they had the capacity to do so. You're going to hear again that there are only excuses that are being offered, that terrorism is really not a serious problem, or that American policy is as terroristic as the policy of al-Qaeda. I don't think you're going to accept that argument.

## IT IS POSSIBLE TO PRESERVE NATIONAL SECURITY WHILE KEEPING BALANCED CONSTRAINTS ON SURVEILLANCE.

Alan Dershowitz, [Harvard University], Debate with Michael Hayden, Alexis Ohanian, and Glenn Greenwald, Toronto, transcript available at The Atlantic, <http://www.theatlantic.com/politics/archive/2014/05/false-equivalence-on-surveillance-from-alan-> dershowitz/361694/, May 5, 2014.

We need to know what harms our enemies, external and internal, are planning in order to prevent them from carrying them out. We also need to impose constraints. And that's why process comes into play. We need a demanding process. But we need to make sure that the burden is realistically designed to strike a proper balance between two equally legitimate but competing values, the need for intelligence to stop attacks against us and the need to protect our privacy from those who place too high a value on security and too low a value on privacy. ¶ I believe it is possible to strike that balance in a manner that protects our freedoms, and that is where our efforts should be directed. Surveillance properly limited and appropriately conducted can promote liberty, protect life, and help us defend our freedoms.

*TERRORISM*

## BIG DATA HELPS TO PREVENT TERRORISM.

Erik J. Dahl, [Assistant Professor of National Security Affairs at the Naval Postgraduate School in Monterey, California], "Discussion Point: It's not Big Data, but Little Data, that Prevents Terrorist Attacks" National Consortium for the Study of Terrorism and Responses to Terrorism, July 25, 2015.

What should we make of all this? It helps to start by understanding how the data collected by the NSA programs may be¶ useful to the U.S. intelligence community. We don’t actually know much about these programs, of course, beyond what has¶ been leaked by Edward Snowden and the claims by intelligence community officials that this data has helped to stop a¶ number of terrorist plots. But from what has been revealed publicly, it seems that these collection programs are useful for¶ what is often the first part of any intelligence effort: gathering a lot more information than is actually needed. This first step is¶ sometimes called a broad area search, as intelligence agencies look in a lot of places, gathering a lot of useless information,¶ before they find the clues that help them narrow the search down to the second step, a focused search for useful, actionable¶ intelligence.¶ This two-step approach was used in the search for Osama bin Laden. After the 9/11 attacks he could have been anywhere,¶ so the intelligence community spent a lot of time running down leads that led to nowhere. But eventually they found the clues¶ that pointed them toward bin Laden’s courier, and that’s where the focused search began, leading them to the compound in¶ Abbottabad, Pakistan.

## NSA PROGRAMS HELP TO PREVENT FUTURE ATTACKS.

Erik J. Dahl, [Assistant Professor of National Security Affairs at the Naval Postgraduate School in Monterey, California], "Discussion Point: It's not Big Data, but Little Data, that Prevents Terrorist Attacks" National Consortium for the Study of Terrorism and Responses to Terrorism, July 25, 2015.

One finding supports the NSA’s argument that the data they are collecting can be useful in preventing future attacks.¶ Opponents have suggested that the NSA data might only be useful in tracking down terrorists after the fact; because those¶ haystacks of information are not apparently being looked at in real time, they are unlikely to help prevent future attacks. But¶ the history of terrorist plots and attacks within the United States since 9/11 shows that most plots take a long time to develop.¶ Even terrorist actions involving only one or two people typically take months or even years to plan and attempt. This is good¶ news, because it gives law enforcement time to discover what’s going on, and it also gives the NSA time to search those¶ haystacks it’s been collecting.

## DIGITAL SURVEILLANCE IS KEY TO SECURITY

Bill Harlow and Marc Theissen, 6/13, [Bill Harlow is a writer, consultant and public relations specialist with over thirty years of experience including assignments in some of the toughest communications positions in the U.S. government. He spent seven years as the top spokesman for the Central Intelligence Agency and four years at the White House handling national security media matters for two Presidents; American author, columnist and political commentator, who served as a speechwriter for United States President George W. Bush and Secretary of Defense Donald Rumsfeld], "Experts Explain Why the NSA Program is Necessary", Secure Freedom Radio, [http://www.centerforsecuritypolicy.org/2013/06/13/arguing-for-the-nsa/.](http://www.centerforsecuritypolicy.org/2013/06/13/arguing-for-the-nsa/)

Edward Snowden’s leak of NSA secrets to the media is reprehensible and as the program stands now the American public has no need for privacy concerns, agree Bill Harlow, former CIA head spokesman, and Marc Thiessen, former speechwriter to President George W. Bush and Secretary of Defense Donald Rumsfeld.¶ On Frank Gaffney’s Secure Freedom Radio show Wednesday, Harlow strongly condemned Snowden’s actions, though he stopped short of calling him a traitor, saying that at the very least Snowden is “clearly a criminal, because he had obligations to protect sensitive information and he decided on his own that he was smarter than everyone in the Executive Branch, all 535 members of Congress, and members of the Judicial Branch in deciding what he could pass on and what he couldn’t.”¶ Thiessen explained that the leaks will cause significant damage to US anti-terror efforts, because “it gives the terrorists information about how we track them, which we don’t want them to posses, and it assists them in their ability to avoid detection…At the same time, you’re discouraging companies from cooperating with the US government…We depend a lot on voluntary cooperation of private businesses in the War on Terror. When their participation is exposed in this way and their international reputations are put at risk and they have outraged calls from stockholders and from customers about this sort of thing, it makes them less likely that they’re going to help us.” The overall effect, Thiessen says, is that “sources and liason partners across the world look at this and say ‘America can’t keep a freakin’ secret.’”¶ Thiessen also stressed how vital the PRISM program and the phone-data collection programs are to national security.¶ “I think we should be celebrating the fact that the NSA is doing this…The fact is we are still facing a terrorist enemy who is trying to attack us. They don’t have armies, navies, and air forces that we can track with satellites. They send 19 men with box cutters to hijack planes and fly them into buildings. So there are only three ways we can find out what their plans are, and in each case they have to tell us. The first case is interrogation. Getting them to tell us their plans. Thanks to Barack Obama we don’t do that any more. Second way to do it is penetration–which is incredibly hard to do–by infiltrating Al Qaeda, either just recruiting double agents or getting someone placed in there….When we have done it we’ve been fooled….So that leaves signaled intelligence. The only way that we have to find out what the terrorists are planning and disrupt their plans is to listen to their communications, monitor their e-mails, monitor them electronically. So if we get rid of this program, if this were to disappear, we would be flying blind.¶ On the initial outcry over the programs made public by the leaks, Harlow says that “Just six weeks ago when the Boston bombings happened many people were saying ‘Why were we let down by the intelligence community? Why didn’t they collect the information that would allow us to stop incidences like that?’ And now just six weeks later we have people crying ‘Why are you trying to connect so

many dots? Why are you trying to get information?’ I think people can be genuinely concerned about the potential invasion of privacy, but you have to also understand that the only way to collect much of this potential information about threats from overseas is to have access to information which may pass through US servers.”¶ Harlow’s ultimate advice is that “to tie our own hands and to destroy a very important collection program on the suspicion that some day somebody might abuse it seem to me a bad way of approaching good government.”

## SURVEILLANCE PROGRAMS ARE CRITICAL COUNTERTERRORISM TOOLS.

The director of the National Security Agency insisted on Tuesday that the government's sweeping surveillance programs have foiled some 50 terrorist plots worldwide in a forceful defense echoed by the leaders of the House Intelligence Committee.¶ Army Gen. Keith Alexander said the two recently disclosed programs – one that gathers U.S. phone records and another that is designed to track the use of U.S.-based Internet servers by foreigners with possible links to terrorism – are critical in the terrorism fight.

## PROGRAMS HAVE ASSISTED THE INTELLIGENCE COMMUNITY TO CONNECT THE DOTS.

Kimberly Dozier, [Associated Press], "NSA: Surveillance Programs Foiled Some 50 Terrorist Plots Worldwide," Huffington Post, June 18, 2013.

Intelligence officials have disclosed some details on two thwarted attacks, and Alexander promised additional information to the panel on thwarted attacks that the programs helped stop. He provided few additional details.¶ The programs "assist the intelligence community to connect the dots," Alexander told the committee in a rare, open Capitol Hill hearing.¶ Alexander got no disagreement from the leaders of the panel, who have been outspoken in backing the programs since Edward Snowden, a 29-year-old former contractor with Booz Allen Hamilton, disclosed information to The Washington Post and the Guardian newspapers.

## SURVEILLANCE PROGRAMS ASSISTED IN THE CAPTURE OF NAJIBULLAH ZAZI

Kimberly Dozier, [Associated Press], "NSA: Surveillance Programs Foiled Some 50 Terrorist Plots Worldwide," Huffington Post, June 18, 2013.

In an online interview with The Guardian in which he posted answers to questions Monday, Snowden said that Zazi could have been caught with narrower, targeted surveillance programs – a point Obama conceded in his interview without mentioning Snowden.¶ "We might have caught him some other way," Obama said. "We might have disrupted it because a New York cop saw he was suspicious. Maybe he turned out to be incompetent and the bomb didn't go off. But, at the margins, we are increasing our chances of preventing a catastrophe like that through these programs," he said.¶ Obama repeated earlier assertions that the NSA programs were a legitimate counterterror tool and that they were completely noninvasive to people with no terror ties – something he hoped to discuss with the privacy and civil liberties board he'd formed. The senior administration official said the president would be meeting with the new privacy board in the coming days.

## NSA SURVEILLANCE PREVENTS TERRORISM

Bucci, Steven. [Dr., Director of The Heritage Foundation's Douglas & Sarah Allison Center for Foreign Policy Studies]. "Phone Records and the NSA: Legal and Keeping America Safe," Heritage Foundation. June 20, 2013, <http://blog.heritage.org/2013/06/20/phone-records-and-the-> nsa-legal-and-keeping-america-safe/

U.S. law enforcement and Intelligence agencies depend on tools and methods, such as the leaked NSA program, to combat homegrown radicalization and to fight the ongoing threat from terrorist cells such as the Al-Qaeda in the Arabian Peninsula in Yemen. Moreover, NSA Director General Keith Alexander testified to Congress that these surveillance programs have helped foil dozens of terrorist attacks. These include, he stated, an attempted suicide plot against the New York City subway system by Najibullah Zazi, who pleaded guilty. Since 9/11, the U.S. has thwarted over 50 terrorist plots against America’s homeland. In addition to continued reliance on counterterrorism devices such as the Patriot Act and the NSA surveillance programs, Congress must take action to plug the remaining gaps in our counterterrorism system. For instance, there should be increased visa coordination to prevent known terrorists from boarding airplanes and travelling to the U.S. Additionally, Congress should foster greater cooperation among local, state, and federal agencies to streamline their information-sharing capabilities. The current debate raging over Snowden’s leaking of the secret NSA surveillance program is no doubt a healthy exercise for a thriving democracy. The scope of the metadata collection and how the government uses it should come under close scrutiny. However, Congress and the American people should understand that these programs—which are under judicial, executive, and legislative oversight— are vital tools for law enforcement and intelligence officials in countering the ongoing threat of terrorism.

## NSA SURVEILLANCE HAS PREVENTED 50 ACTS OF TERRORISM

Bucci, Steven. [Dr., Director of The Heritage Foundation's Douglas & Sarah Allison Center for Foreign Policy Studies]. "NSA Spying Stops Terrorism but Should Also Respect Liberties," Heritage. June 18, 2013, <http://blog.heritage.org/2013/06/18/nsa-spying-stops-terrorism-but-> should-also-respect-liberties/

General Keith Alexander, the director of the National Security Agency (NSA), testified in an open hearing before the House Permanent Select Committee for Intelligence on how intelligence collection supports the national effort to fight transnational terrorism. For the first time, he revealed that more than 50 incidents of potential terrorism were stopped by the set of programs under scrutiny. He emphasized that he was working to declassify these incidents so they could be shared with the American people. These revelations come as no surprise to us. Heritage research has noted 54 foiled terrorist plots since 9/11. Given that we know of only three that were not stopped by intelligence (the shoe bomber, the underwear bomber, and the Times Square bomber), this means that these NSA programs might well have played a significant role in thwarting dozens of uncovered plots. Heritage has long held that tools such as the PATRIOT Act and legitimate surveillance programs can be important tools for battling transnational terrorism.

## DIGITABLE SURVEILLANCE IS NECESSARY FOR EFFECTIVE COUNTERROR EFFORTS

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012,<http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-> antique-privacy-rules

Cyberspace is the natural battleground for enhanced analytical tools that are enabled by the technology of data collection. If our goal is to combat terrorists or insurgents (or even other nations) then the cyber domain offers us the capacity not just to steal secret information through espionage, but to take observable public behavior and information and use cyber tools to develop a more nuanced and robust understanding of their tactics and intentions. Likewise, it can be used by our opponents to uncover our own secrets. Traditionally, the concept of “surveillance” has been taken to mean an act of physical surveillance—e.g., following someone around or planting a secret camera in an apartment. As technology improved, our spy agencies and law enforcement institutions increasingly came to rely on even more sophisticated technical means of surveillance,[5] and so we came to develop the capacity to electronically intercept telecommunications and examine email while in transit.[6] To these more “traditional” forms of surveillance we must now add another: the collection and analysis of personal data and information about an individual or organization. Call the phenomenon “dataveillance” if you wish, but it is an inevitable product of our increasing reliance on the Internet and global communications systems. One leaves an electronic trail almost everywhere you go. Increasingly, in a networked world technological changes have made personal information pervasively available. As the available storehouse of data has grown, so have governmental and commercial efforts to use this personal data for their own purposes. Commercial enterprises target ads and solicit new customers. Governments use the data to, for example, identify and target previously unknown terror suspects—to find so-called clean skins who are not in any intelligence database. This capability for enhanced data analysis has already proven its utility and holds great promise for the future of commercial activity and counter-terrorism efforts.

## THE DATA IS VERY HELPFUL TO INVESTIGATIONS

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012,<http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-> antique-privacy-rules

Compare that condemnation with the universal criticism of the government for its failure to “connect the dots” during the Christmas 2009 bomb plot attempted by Umar Farouk Abdulmutallab.[8] This gives you some idea of the crosscurrents at play. The conundrum arises because the analytical techniques are fundamentally similar to those used by traditional law enforcement agencies, but they operate on so much vaster a set of data, and that data is so much more readily capable of analysis and manipulation, that the differences in degree tend to become differences in kind. To put the issue in perspective, just consider a partial listing of relevant databases that might be targeted: credit card, telephone calls, criminal records, real estate purchases, travel itineraries, and so on. One thing is certain—these analytical tools are of such great utility that governments will expand their use, as will the private sector. Old rules about collection and use limitations are no longer technologically relevant. If we value privacy at all, these ineffective protections must be replaced with new constructs. The goal then is the identification of a suitable legal and policy regime to regulate and manage the use of mass quantities of personal data.

## SURVEILLANCE IS CRITICAL TO PREVENTING TERRORIST ATTACKS

Zuckerman, Jessica [Policy Analyst, Western Hemisphere at Heritage Foundation]. "60 Terrorist Plots Since 9/11: Continued Lessons In Domestic Counterterrorism," The Heritage Foundation. July 31, 2013, <http://www.heritage.org/research/commentary/2013/7/60-terrorist-plots-since-911-> continued-lessons-in-domestic-counterterrorism

Maintain essential counterterrorism tools. Support for important investigative tools such as the PATRIOT Act is essential to maintaining the security of the U.S. and combating terrorist threats. Key provisions within the act, such as the roving surveillance authority and business records provision, have proved essential for thwarting terror plots, yet they require frequent reauthorization. In order to ensure that law enforcement and intelligence authorities have the essential counterterrorism tools they need, Congress should seek permanent authorization of the three sun setting provisions within the PATRIOT Act.[208] Furthermore, legitimate government surveillance programs are also a vital component of U.S. national security, and should be allowed to continue. Indeed, in testimony before the house, General Keith Alexander, the director of the National Security Agency (NSA), revealed that more than 50 incidents of potential terrorism at home and abroad were stopped by the set of NSA surveillance programs that have recently come under scrutiny. That said, the need for effective counterterrorism operations does not relieve the government of its obligation to follow the law and respect individual privacy and liberty. In the American system, the government must do both equally well.

## SURVEILLANCE EMPIRICALLY PREVENTS ATTACKS ON THE HOMELAND

Zuckerman, Jessica [Policy Analyst, Western Hemisphere at Heritage Foundation]. "60 Terrorist Plots Since 9/11: Continued Lessons In Domestic Counterterrorism," The Heritage Foundation. July 31, 2013, <http://www.heritage.org/research/commentary/2013/7/60-terrorist-plots-since-911-> continued-lessons-in-domestic-counterterrorism

At 2:50 p.m. on April 15, 2013, two explosions went off at the finish line of the Boston Marathon. The brazen terrorist attack killed three people, injured and maimed hundreds more, and shocked the nation. Despite being long recognized as a potential threat by law enforcement and intelligence, few Americans had considered the use of an improvised explosive device (IED) on American soil. And, due to only a few, and relatively small, attacks since 9/11, the public was not in a state of awareness. Yet, the fact remains that there have been at least 60 Islamist-inspired terrorist plots against the homeland since 9/11, illustrating the continued threat of terrorism against the United States. Fifty-three of these plots were thwarted long before the public was ever in danger, due in large part to the concerted efforts of U.S. law enforcement and intelligence. The Heritage Foundation has tracked the foiled terrorist plots against the United States since 9/11 in an effort to study the evolving nature of the threat and garner lessons learned. The best way to protect the United States from the continued threat of terrorism is to ensure a strong and capable domestic counterterrorism enterprise—and to understand the continuing nature of the terror threat.

## SURVEILLANCE IS THE LAST, BEST DEFENSE AGAINST TERRORISM

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "Big Brother isn’t watching you," American Enterprise Institute. June 10, 2013, <http://aei.org/article/foreign-and-defense-policy/terrorism/big-brother-isnt-watching-you/>

If the critics don’t think the NSA should be collecting this information, perhaps they would like to explain just how they would have us stop new terrorist attacks. Terrorists don’t have armies or navies we can track with satellites. There are only three ways we can get information to prevent terrorist attacks: The first is interrogation — getting the terrorists to tell us their plans. But thanks to Barack Obama, we don’t do that anymore. The second is penetration, either by infiltrating agents into al-Qaeda or by recruiting operatives from within the enemy’s ranks. This is incredibly hard — and it got much harder, thanks to the leak exposing a double agent, recruited in London by British intelligence, who had penetrated al-Qaeda in the Arabian Peninsula and helped us break up a new underwear bomb plot in Yemen — forcing the extraction of the agent. That leaves signals intelligence — monitoring the enemy’s phone calls and Internet communications — as our principal source of intelligence to stop terrorist plots. Now the same critics who demanded Obama end CIA interrogations are outraged that he is using signals intelligence to track the terrorists.

Well, without interrogations or signals intelligence, how exactly is he supposed to protect the country? Unfortunately, some on the right are joining the cacophony of condemnation from the New York Times and MSNBC. The programs exposed in these leaks did not begin on Barack Obama’s watch. When Obama continues a Bush-era counterterrorism policy, it is not an outrage

— it is a victory.

## SURVEILLANCE IS NEEDED TO PREVENT TERRORISM

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "Yes, publishing NSA secrets is a crime," American Enterprise Institute. June 17, 2013,<http://aei.org/article/foreign-and-defense-policy/defense/intelligence/yes-publishing-nsa-secrets-> is-a-crime/

Many do not realize it, but the law is much stricter with the disclosure of signals intelligence than it is with the disclosure of other classified information. All leaks of classified information are damaging, but the exposure of signals intelligence can be catastrophic. Just think back to World War II. If someone had compromised a human intelligence source, a spy or double agent who had infiltrated the Nazi high command, that asset could lose his life, but we would have lost a relatively small amount of intelligence. But if someone had exposed the allies’ top secret ULTRA program — through which we broke the encrypted radio and telegraphic codes used by the Nazi leadership — it could very well have altered the outcome of the war. Signals intelligence is of similar import in the war on terror. We cannot track small terrorist cells with spy satellites. The only way we can disrupt the terrorists’ plans is by getting them to tell us their plans. In the

absence of interrogation, one of the only ways to do that is through signals intelligence. That is why the NSA’s surveillance activities are so essential — and why Greenwald could face prosecution for exposing them.

## SURVEILLANCE PROVIDES INFORMATION TO PREVENT A FUTURE 9/11

Yoo, John. [Law Professor at the University of California, Berkeley]. "Why We Endorsed Warrantless Wiretaps," American Enterprise Institute. July 16, 2009, <http://aei.org/article/foreign-> and-defense-policy/defense/why-we-endorsed-warrantless-wiretaps/

It was instantly clear after Sept. 11, 2001, that our security agencies knew little about al Qaeda's inner workings, could not detect its operatives' entry into the country, nor predict where it might strike next. Suppose an al Qaeda cell in New York, Chicago or Los Angeles was planning a second attack using small arms, conventional explosives or even biological, chemical or nuclear weapons. Our intelligence and law enforcement agencies faced a near impossible task locating them. Now suppose the National Security Agency (NSA), which collects signals intelligence, threw up a virtual net to intercept all electronic communications leaving and entering Osama bin Laden's Afghanistan headquarters. What better way of detecting follow-up attacks? And what president--of either political party--wouldn't immediately order the NSA to start, so as to find and stop the attackers? Evidently, none of the inspectors general of the five leading national security agencies would approve. In a report issued last week, they suggested that President George W. Bush might have violated the 1978 Foreign Intelligence Surveillance Act (FISA) by ordering the interception of international communications of terrorists without a judicial warrant. The report also suggests that "other" intelligence measures--still classified only because they are yet to be reported on the front page of the New York Times--similarly lacked approval from other branches of government. It is absurd to think that a law like FISA should restrict live military operations against potential attacks on the United States. Congress enacted FISA during the waning days of the Cold War. As the 9/11 Commission found, FISA's wall between domestic law enforcement and foreign intelligence proved dysfunctional and contributed to our government's failure to prevent the 9/11 attacks.

## TERRORISM IS A REAL THREAT - SURVEILLANCE IS REQUIRED TO DEFEAT IT

Yoo, John. [Law Professor at the University of California, Berkeley]. "Privacy or Protection?," The American Enterprise Institute. February 11, 2007, <http://aei.org/article/foreign-and-defense-> policy/terrorism/privacy-or-protection/

Our political leaders should consider new ways of addressing this new type of threat. The NSA's terrorist surveillance program, which seeks to intercept communications into or out of the United States involving a suspected al Qaeda agent, represents an effort to go beyond the terrorism-as- crime approach. Preventing terrorist attacks depends on spotting, in advance, patterns and connections in communications, travel and transfers of funds, rather than for waiting for the attacks to occur. We must allow our intelligence agencies to connect the dots, to gather more data, search more broadly, and pool information among more analysts and agencies. Once it was safe to assume there was little need for any domestic surveillance because we no longer faced any serious communist threat; instead, such activities imperiled the privacy rights of harmless students and protesters. The al Qaeda threat is not imaginary, nor an artifact of history, nor a distant or attenuated concern--it is quite real.

## SURVEILLANCE WOULD HAVE PREVENTED 9/11

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "The John Kerry Republicans," Washington Post. July 29, 2013, <http://www.washingtonpost.com/opinions/marc-thiessen-house-republicans-nsa-> hypocrisy/2013/07/29/a39612f8-f847-11e2-8e84-c56731a202fb\_story.html

The fact is, they were right the first time. The NSA asked Congress to approve the telephone metadata program in order to close a specific gap in our intelligence capabilities — one that made the 9/11 attacks possible. In the summer of 2001, the NSA had intercepted calls from two of the 9/11 hijackers — Nawaf al-Hazmi and Khalid al-Mihdhar — to an al-Qaeda safe house in the Middle East whose communications were being monitored. However, because the NSA did not have access to metadata on U.S. telephone calls, intelligence officials had no way to know that the two hijackers were in the United States and that their calls had originated in San Diego. As former NSA director Mike Hayden recently pointed out, “If the metadata program had been in effect in the summer of 2001, al-Hazmi and al-Mihdhar would likely have been rolled up, the plane that hit the Pentagon would not have had these jihadists available for the hijacking, and the entire 9/11 enterprise might have been scrapped by al-Qaeda.”

## ERR ON THE SIDE OF EXPANSIVE INTELLIGENCE PROGRAMS

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "The John Kerry Republicans," Washington Post. July 29, 2013, <http://www.washingtonpost.com/opinions/marc-thiessen-house-republicans-nsa-> hypocrisy/2013/07/29/a39612f8-f847-11e2-8e84-c56731a202fb\_story.html

After 9/11, the House and Senate intelligence committees conducted a joint inquiry into the intelligence failures that led to the attacks. They concluded that one of the main culprits was the “NSA’s cautious approach to any collection of intelligence relating to activity in the United States.” Now, after a dozen years without an attack on the homeland, they are being accused of the opposite offense. When terrorist attacks succeed, members of Congress are the first to demand that intelligence officials explain why they failed to “connect the dots.” Well, if Congress ends the metadata program, those intelligence officials will have a simple answer: because you took away the field of dots.

## TERRORISTS WANT TO ATTACK THE US BUT SURVEILLANCE EFFORTS STOP THEM

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013,<http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

After 9/11, there was a widespread expectation of many more terrorist attacks on the United States. So far that hasn't happened. We haven't escaped entirely unscathed (see Boston Marathon, bombing of), but on the whole we have been a lot safer than most security experts, including me, expected. In light of the current controversy over the National Security Agency's monitoring of telephone calls and emails, it is worthwhile to ask: Why is that? It is certainly not due to any change of heart among our enemies. Radical Islamists still want to kill American infidels. But the vast majority of the time, they fail. The Heritage Foundation estimated last year that 50 terrorist attacks on the American homeland had been foiled since 2001. Some, admittedly, failed through sheer incompetence on the part of the would-be terrorists. For instance, Faisal Shahzad, a Pakistani American jihadist, planted a car bomb in Times Square in 2010 that started smoking before exploding, thereby alerting two New Yorkers who in turn called police, who were able to defuse it.

## ABSENT NSA SURVEILLANCE, THERE WOULD HAVE BEEN MORE ATTEMPTED ATTACKS

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013,<http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

But it would be naive to adduce all of our security success to pure serendipity. Surely more attacks would have succeeded absent the ramped-up counter-terrorism efforts undertaken by the

U.S. intelligence community, the military and law enforcement. And a large element of the intelligence community's success lies in its use of special intelligence — that is, communications intercepts. The CIA is notoriously deficient in human intelligence — infiltrating spies into terrorist organizations is hard to do, especially when we have so few spooks who speak Urdu, Arabic, Persian and other relevant languages. But the NSA is the best in the world at intercepting communications. That is the most important technical advantage we have in the battle against fanatical foes who will not hesitate to sacrifice their lives to take ours.

## SURVEILLANCE SYSTEMS EXIST BECAUSE THEY WORK

Foust, Joshua. [Fellow at the American Security Project]. "These Programs Exist Because They Work," The New York Times. June 10, 2013,<http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-> imagined

While debating the morality and ultimate legality of last week’s N.S.A. revelations is important, it is also important to realize why programs like collecting telephone metadata and Prism exist to begin with. In short: people think it works. News stories from 2002 show that the public was demanding the intelligence community “do more” to analyze information and thwart any future terrorist attacks. As a result, many of the barriers between domestic law enforcement and intelligence agencies, built after the 1975 Church Committee hearings, have been removed to make investigations easier. Has removing the “wall” actually helped to prevent terrorist attacks? Anonymous government sources have advanced the claim that Prism – a workflow management tool misreported as a means for collecting information – was instrumental in stopping Najibullah Zazi, who had planned on bombing the New York subway system. Those claims are disputed, at least in part, by public records of the Zazi case.

*AT ABUSE OF POWER*

## THE NSA IS AN ACCOUNTABLE PROGRAM

**Page 96 of 176**

Carroll, Conn. [senior writer for the Washington Examiner]. "Two Steps Back for National Security," The Heritage Foundation. March 12, 2008, <http://blog.heritage.org/2008/03/12/two-> steps-back-for-national-security/

The abject scaremongering by the left on “the NSA’s warrantless domestic spying” is not supported by any facts. The details of the program in question have not, and should not, be revealed. But from what we can piece together from the public record, the program in question touched domestic communications only incidentally and there is zero evidence anywhere that anyone innocent Americans have had their telephone calls listened to or their emails read. FISA experts have made it clear the NSA program in question was probably targeted at electronic communications like email. Due to the complexity and interconnectedness of modern communications, it is impossible for telecommunication companies, or the NSA, to instantly determine whether a single packet of information traveling through a wire in the U.S. is purely foreign in nature (someone in Baghdad e-mailing someone in Riyadh) or purely domestic. The NSA uses complex algorithms to determine if a communication if foreign or domestic, but they first require cooperation from a telecommunication company to keep that data.

## THERE ARE INTERNAL CHECKS ON PRIVACY LOSS

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012,<http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-> antique-privacy-rules

First, we are changing from a top-down process of command and control rule to one in which the principal means of privacy protection is through institutional oversight. To that end, the Department of Homeland Security was created with a statutorily required Privacy Officer (and another Officer for Civil Rights and Civil Liberties).[46] The more recent Intelligence Reform and Terrorism Prevention Act,[47] and the Implementing Recommendations of the 9/11 Commission Act of 2007[48] go further. For the first time, they created a Civil Liberties Protection Officer within the intelligence community. More generally, intelligence activities are to be overseen by an independent Privacy and Civil Liberties Oversight Board.[49] Indeed, these institutions serve a novel dual function. They are, in effect, internal watchdogs for privacy concerns. In addition, they naturally serve as a focus for external complaints, requiring them to exercise some of the function of ombudsmen. In either capacity, they are a new structural invention on the American scene—at least, with respect to privacy concerns. Second, and perhaps most significantly, the very same dataveillance systems that are used to advance our counter-terrorism interests are equally well suited to assure that government officials comply with the limitations imposed on them in respect of individual privacy. Put another way, the dataveillance systems are uniquely well equipped to watch the watchers, and the first people who should lose their privacy are the officials who might wrongfully invade the privacy of others.

## SURVEILLANCE IS LAWFUL AND EFFECTIVE

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "Big Brother isn’t watching you," American Enterprise Institute. June 10, 2013, <http://aei.org/article/foreign-and-defense-policy/terrorism/big-brother-isnt-watching-you/>

But instead of being outraged by the damage done by these leaks, critics on the left and right are criticizing the NSA for undertaking activities that are lawful, constitutional and absolutely vital to protecting the country. Calm down, folks. Big Brother is not watching you. During the Bush administration, critics opposed what they called “warrantless wiretapping.” Well, the leaked NSA operations are not warrantless. And, in the case of Verizon, they do not even involve wiretapping. The Verizon court order shows that what is being tracked is not the content of the communications but the records of which phone number called which number, as well as the location and duration of the calls. In Smith v. Maryland , the Supreme Court held that there’s no reasonable expectation of privacy, and thus no Fourth Amendment protection, for the phone numbers people dial (as distinct from the content of the call), because the number dialed is information you voluntarily share with the phone company to complete the call and for billing purposes. Why does the NSA need to collect all that data? One former national security official explained it to me this way: If you want to connect the dots and stop the next attack, you need to have a “field of dots.” That is what the NSA is collecting. But it doesn’t dip into that field unless it comes up with a new “dot” — for example, a new terrorist phone number found on a cellphone captured in a raid. It will then plug that new “dot” into the “field of dots” to find out which dots are connected to the new number. If you are not communicating with that terrorist, your dot is not touched. But the NSA needs to have the entire field of dots so it can unravel the network connected to that terrorist. In the case of the PRISM program, the NSA is targeting foreign nationals, not U.S. citizens, and not even individuals in the United States. And all of this collection is being done with a warrant, issued by a federal judge, under authorities approved by Congress.

## THERE IS NO EVIDENCE OF PROGRAM ABUSE

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013,<http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

At first blush these intelligence-gathering activities raise the specter of Big Brother snooping on ordinary American citizens who might be cheating on their spouses or bad-mouthing the president. In fact, there are considerable safeguards built into both programs to ensure that doesn't happen. The phone-monitoring program does not allow the NSA to listen in on conversations without a court order. All that it can do is to collect information on the time, date and destination of phone calls. It should go without saying that it would be pretty useful to know if someone in the U.S. is calling a number in Pakistan or Yemen that is used by a terrorist organizer. As for the Internet-monitoring program, reportedly known as PRISM, it is apparently limited to "non-U.S. persons" who are abroad and thereby enjoy no constitutional protections.

These are hardly rogue operations. Both programs were initiated by President George W. Bush and continued by President Obama with the full knowledge and support of Congress and continuing oversight from the federal judiciary. That's why the leaders of both the House and Senate intelligence committees, Republicans and Democrats alike, have come to the defense of these activities. It's possible that, like all government programs, these could be abused — see, for example, the IRS making life tough on tea partiers. But there is no evidence of abuse so far and plenty of evidence — in the lack of successful terrorist attacks — that these programs have been effective in disrupting terrorist plots.

## ABUSE CONCERNS ARE ENTIRELY BASELESS

Posner, Eric. [Law professor at the University of Chicago]. "I Don’t See a Problem Here," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-> surveillance-threat-real-or-imagined

The second objection is a lot more serious. We know that our government is capable of misusing information in this way, as occurred during the Nixon administration. Many people seem to believe that President Obama sent telepathic signals to I.R.S. workers instructing them to harass Tea Party organizations. But I am unaware — and correct me if I am wrong — of a single instance during the last 12 years of war-on-terror-related surveillance in which the government used information obtained for security purposes to target a political opponent, dissenter or critic. That means that, for now, this objection is strictly theoretical, and the mere potential for abuse can’t by itself be a good reason to shut down a program. If it were, we would have no government.

## THERE IS LEGAL PRECEDENT FOR THE NSA’S ACTIONS.

Roger Pilon [Vice President for legal affairs at the Cato Institute] and Richard A. Epstein [Law Professor at New York University Law School], "NSA Surveillance in Perspective," Cato Institute, June 12, 2013.

In 1979, in Smith v. Maryland, the U.S. Supreme Court addressed that balance when it held that using a pen register to track telephone numbers did not count as an invasion of privacy, even in ordinary criminal cases. That’s just what the government is doing here on a grand scale. The metadata it examines in its effort to uncover suspicious patterns enables it to learn the numbers called, the locations of the parties, and the lengths of the calls. The government does not know — as some have charged — whether you’ve called your psychiatrist, lawyer or lover. The names linked to the phone numbers are not available to the government before a court grants a warrant on proof of probable cause, just as the Fourth Amendment requires. Indeed, once that warrant is granted to examine content, the content can be used only for national security issues, not even ordinary police work.

## THE OBAMA ADMINISTRATION IS ON SECURE LEGAL FOOTING.

Roger Pilon [Vice President for legal affairs at the Cato Institute] and Richard A. Epstein [Law Professor at New York University Law School], "NSA Surveillance in Perspective," Cato Institute, June 12, 2013.

Legally, the president is on secure footing under the Patriot Act, which Congress passed shortly after 9/11 and has since reauthorized by large bipartisan majorities. As he stressed, the program has enjoyed the continued support of all three branches of the federal government. It has been free of political abuse since its inception. And as he rightly added, this nation has real problems if its people, at least here, can’t trust the combined actions of the executive branch and the Congress, backstopped by federal judges sworn to protect our individual liberties secured by the Bill of Rights.

## NSA SURVEILLANCE DOES NOT VIOLATE THE FOURTH AMENDMENT.

Orin Kerr, [Professor of criminal procedure and computer crime law at George Washington University], "My defense of the third-party doctrine and a response to Randy and Stewart," Washington Post, May 5, 2014.

I appreciate Randy’s consistent application of his “unprecedented” principle of constitutional interpretation from the Obamacare case. With that said, I don’t think this argument works very well. First, the Fourth Amendment doesn’t prohibit unreasonable things generally. Based on its text, it only prohibits unreasonable searches and seizures. The scope of a search or seizure goes to its reasonableness, as the example of general warrants indicates. But if government conduct is not a search or seizure, then its reasonableness isn’t relevant to its constitutionality. This is important because Smith v. Maryland held that obtaining numbers dialed was not a search. Given that, I don’t think one can plausibly distinguish Smith on reasonableness grounds. I should also note, contrary to Randy’s claim, that the government did not obtain a specific court order in Smith. Congress did not require a court order for pen registers until 1986, seven years after the Supreme Court’s decision. As a result, there was no court order in Smith. The Supreme Court approved surveillance with no judicial oversight, not surveillance pursuant to particular court orders.¶ Finally, I agree with Stewart Baker that the line-drawing problem once you reject Smith

v. Maryland poses a major problem for Smith‘s critics. I wrote about that at length here and here. In my experience, critics of Smith don’t have much of a response. For example, in our debate on the third-party doctrine, NYU lawprof Erin Murphy had a particularly candid reply to the problem of what would replace Smith: “Truthfully, I have no idea.” I think that’s a problem. If Fourth Amendment scholars who strongly oppose Smith themselves don’t know what should replace it, the need to come up with an alternative should at least give some pause to generalist judges faced with the problem for the first time.

*AT MOTIVES*

## NSA SURVEILLANCE ISN’T BASED ON ULTERIOR MOTIVES.

Alan Dershowitz, [Harvard University], Debate with Michael Hayden, Alexis Ohanian, and Glenn Greenwald, Toronto, transcript available at The Atlantic, <http://www.theatlantic.com/politics/archive/2014/05/false-equivalence-on-surveillance-from-alan-> dershowitz/361694/, May 5, 2014.

So I will throw out a challenge out to our distinguished opponents. ¶ What are those motives? Why would the Obama Administration continue this policy of surveillance after being briefed? Was it because President Obama has some sinister motive that he won't tell anybody about for gathering this information and is only using terrorism as a pretext the way the Nazis in Germany used the Reichstag fire as a way of suppressing civil liberties? I don't believe that. ¶ I hope you won't either. ¶ Motives matter, though they too are difficult to discern and are frequently mixed. Many who supported the surveillance conducted by the FBI against the Ku Klux Klan and other racist groups during the civil-rights movement opposed the very same surveillance techniques when they were used years later against the Black Panthers. And many who now applaud the decision to publish the illegally recorded private statements made by Donald Sterling to his mistress would express outrage if equally pernicious statements made in private by people they admire and respect were subject to public disclosure. Privacy for me but not for thee is as common as it is cynically self-serving. Now we ought to be concerned about surveillance. There's virtually nothing that's immune from the pervasive eyes, ears and even noses of the new generation of Big Brothers. It's absolutely true. But the most dangerous approach to our liberties is the all or nothing one proposed by radical proponents and opponents of all government surveillance. Those who oppose all surveillance are as dangerous to our liberties as those who uncritically support all surveillance.

## NEW NSA CHIEF WILL IMPROVE TRANSPARENCY.

PressTV, "NSA Chief Defends Surveillance Programs," [http://www.presstv.ir/detail/2014/05/13/362422/nsa-chief-defends-surveillance-programs/,](http://www.presstv.ir/detail/2014/05/13/362422/nsa-chief-defends-surveillance-programs/) May 13, 2014.

He also vowed to lead the spy agency with greater transparency. Rogers said he had told the rank and file at the NSA that they should keep on as before, but come forward internally with anything they felt to be improper.¶ "It is by design that I have tried to start a series of engagements with a broader and perhaps more different groups than we have traditionally done," Rogers told the Reuters Cybersecurity Summit in Washington.¶ "The dialogue to date that we have had for much of the last nine months or so from my perspective, I wish was a little bit broader, had a little more context to it, and was a little bit more balanced."¶

## IMPROVED TRANSPARENCY WON’T HINDER THE NSA.

John Mueller [political scientist at Ohio state] and Mark G. Stewart [civil engineer at the University of Newcastle in Australia], "Three Questions about NSA Surveillance," Cato Institute, June 13, 2013.

It is difficult to see how earlier exposure of the programs’ existence would have aided terrorists, who have known at least since the 1990s that U.S. intelligence was searching communications worldwide to track them down. It is possible, however, that the secrecy of the programs stems from the Obama administration’s fear that public awareness of “modest encroachments” on privacy would make further efforts to encroach more difficult.¶ A former Air Force secretary told Reuters that a “growing unease about domestic surveillance could have a chilling effect on proposed cyber legislation that calls for greater information-sharing between government and industry.” Since the revelation, more lawmakers have signed on to legislation that would strengthen the privacy protections in the 1986 Electronic Communications Privacy Act. The notion here, then, is that the programs were secret not to protect people from terrorism, but to protect the government from inconvenient public and Congressional opposition.

# NEGATIVE EVIDENCE

*DEFINITIONS*

## PRIVACY DEFINITION

Nikki Gulzar et al, [Auckland University of Technology], "Surveillance Privacy Protection," [http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf,](http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf) 2013.

Whenever we are under surveillance, privacy becomes an issue. Privacy has been commonly used within western society, however, it was not a general concept and to many cultures it was virtually unknown, until recently [95]. Privacy is an indi- vidual right to control what happens with personal data [71, 102]. The meaning of privacy may differ throughout cultures but the general conception is that privacy means wanting to keep information unnoticed or unidentified from the general pub- lic. Privacy can be categorized in different contexts [35, 65].

## PRIVACY INVOLVES PERSONAL AND PHYSICAL PRIVACY

Nikki Gulzar et al, [Auckland University of Technology], "Surveillance Privacy Protection," [http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf,](http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf) 2013.

Personal privacy is one of the first issues that are being violated. Personal privacy allows an individual to keep their body or beliefs private. Physical privacy can be defined as preventing intrusion into one’s personal space or solitude. The concerns may be [59]:¶ • Not allowing personal possessions searched by an unwelcome party¶ • Not allowing access to people’s homes and vehicle without authorization¶ Most countries have trespassing and property rights which help to determine the right to physical properties [44].

## DIGITAL PRIVACY DEFINITION

Nikki Gulzar et al, [Auckland University of Technology], "Surveillance Privacy Protection," [http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf,](http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf) 2013.

Data privacy is the second most important issue when it comes to privacy. We all want to secure our personal data but data privacy is about an evolving relationship between technology and legal rights, which makes it harder to keep data private. The data storage causes some privacy issues such as who will access to the data, how the data is stored and the user’s rights for protection [67]. There are some web sites that ask for more data than necessary but it is unclear as to what they share. Privacy issues especially to personal data include insecure, electronic transmission, data trails and logs of email messages, and the tracking of web pages visited [102]. Nowadays every kind of organization is marketing online users, which means that we are putting more of our personal data online and sometimes it becomes hard to keep track of all the information. Without our knowledge, the data could be sold to make profits [39, 47]. Therefore data privacy has become very important, it gives us a little control over the information we share, and the penalty for privacy violation has become more severe.

## ORGANIZATIONAL PRIVACY DEFINITION

Nikki Gulzar et al, [Auckland University of Technology], "Surveillance Privacy Protection," [http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf,](http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf) 2013.

Organizational privacy allows government agencies or organizations to keep their activities private and prevent it from being leaked to other organizations. Each or- ganization has its own privacy policy, which helps them to maintain the privacy of personal data. An example of the organizational privacy is internet privacy. When organizations have web interactions for their customers, they must take customers’ right into consideration when it comes to their personal data [26]. Data Privacy Day is about empowering people to protect their privacy and control their digital foot- prints to ensure the protection of data privacy [4].

## PRIVACY DEFINITION

James Waldo et al, [Sun Microsystems], "Thinking About Privacy: Chapter 1 of "Engaging Privacy and Information Technology in a Digital Age" Journal of Privacy and Confidentiality, 2010.

The committee began by trying to understand what privacy is, and it quickly found that privacy is an ill-defined but apparently well-understood concept. It is ill-defined in the sense that people use the term to mean many different things. Any review of the literature on privacy will reveal that privacy is a complicated concept that is difficult to define at a theoretical level under any single, logically consistent “umbrella” theory, even if there are tenuous threads connecting the diverse meanings. Specifying the concept in a way that meets with universal consensus is a difficult if not impossible task, as the committee found in doing its work.¶ At the same time, the term “privacy” is apparently well understood in the sense that most people using the term believe that others share their particular definition. Nonetheless, privacy resists a clear, concise definition because it is experienced in a variety of social contexts. For example, a question may be an offensive privacy violation in one context and a welcome intimacy in another.¶ The committee believes that in everyday usage, the term “privacy” generally in- cludes reference to the types of information available about an individual, whether they are primary or derived from analysis. These types of information include behavioral, financial, medical, biometric, consumer, and biographical. Privacy interests also attach to the gathering, control, protection, and use of information about individuals. Infor- mational dimensions of privacy thus constitute a definitional center of gravity for the term that is used in this report, even while recognizing that the term may in any given instance entail other dimensions as well—other dimensions that are recognized explicitly in the discussion.2

## PROGRAM ABUSE HAS HAPPENED BEFORE AND WILL CONTINUE

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Privacy Is Worth Protecting," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-> imagined

You say you are unaware of a single instance, since 9/11, in which the government used surveillance to target a political opponent, dissenter or critic. But if the government were using surveillance this way, would officials tell us? So much secrecy surrounds the government’s surveillance activities that we simply don’t know how often, or in what ways, the government’s surveillance powers have been abused. This said, we know enough that we ought to be worried. Here is an article about the Department of Homeland Security conducting inappropriate surveillance of protesters associated with Occupy Wall Street. Here is a report of the Justice Department’s inspector general finding that the F.B.I. monitored a political group because of its anti-war views. Here is a story in which a former C.I.A. official says that the agency gathered information about a prominent war critic “in order to discredit him.”’

## PROGRAM ABUSE IS INEVITABLE

Goldberg, Jonah. [contributing editor to National Review, named by the Atlantic magazine as one of the top 50 political commentators in America]. "Civil libertarians' hypocrisy," American Enterprise Institute. July 8, 2013, <http://aei.org/article/politics-and-public-opinion/civil-libertarians-> hypocrisy/

"At least 850,000 people have security clearances that give them access to this information," Tiffiniy Cheng of Fight for the Future recently wrote on The Huffington Post. "That's the size of Boston. Imagine if they leak information about a politician or business leaders' personal life — what about a prominent activist? The opportunities for abuse and blackmail are endless; despite what some members of Congress have claimed, the history of government surveillance programs is riddled with abuses." Farhad Manjoo of online Slate magazine agrees. The "fundamental problem" with the NSA's surveillance program is that it's amassing an all-too-tempting stockpile of information. "Someone has access to that data, and that someone might not be as noble as (Edward) Snowden. He could post everything online. He could sell it to identity thieves. He could blackmail you. Or he might blackmail politicians, businesspeople, judges, TSA agents, or use the data in some other nefarious way." One needn't be a privacy absolutist, never mind a paranoid conspiracy theorist, to believe that this is a legitimate concern. One can even support the NSA's PRISM program and still want significant safeguards against abuse.

## SURVEILLANCE INEVITABLY BLEEDS INTO DISCRIMINATION AND PROFILING

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013),<http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf>

From one perspective, the use of the fruits of data surveillance in this way might look like ordinary marketing. But consider the power that data-driven marketing gives companies in relation to their customers. The power of sorting can bleed imperceptibly into the power of discrimination. A coupon for a frequent shopper might seem innocuous, but consider the power to offer shorter airport security lines (and less onerous procedures) to rich frequent fliers, or to discriminate against customers or citizens on the basis of wealth, geography, gender, race, or ethnicity. The power to treat people differently is a dangerous one, as our many legal rules in the areas of fair credit, civil rights, and constitutional law recognize. Surveillance, especially when fuelled by Big Data, puts pressure on those laws and threatens to upend the basic power balance on which our consumer protection and constitutional laws operate. As Professor Danielle Citron argues, algorithmic decisionmaking based on data raises issues of “technological due process.”116 The sorting power of surveillance only raises the stakes of these issues. After all, what sociologists call “sorting” has many other names in the law, with “profiling” and “discrimination” being just two of them.

## CANADA AIDS THE NSA IN SURVEILLANCE.

Peter Edwards, [Star Reporter], "Canada actively spies for NSA, Glenn Greenwald claims in new book," The Star, <http://www.thestar.com/news/canada/2014/05/13/canada_actively_spies_for_nsa_new_book_say> s.html, May 13, 2014.

“The hacking practice is quite widespread in its own right: one NSA document indicates that the agency had succeeded in infecting at least fifty thousand individual computers with a type of malware called Quantum insertion,” writes Greenwald, a member of the team from The Guardian which, along with The Washington Post, were awarded the 2014 Pulitzer Prize in public service.¶ Quoting from a top secret April 2013 NSA information paper, Greenwald writes: “There is evidence of widespread CSEC/NSA co-operation, including Canada’s efforts to set up spying posts for communications surveillance around the world at the behest and for the benefit of the NSA, and spying on trading partners targeted by the U.S. agency.”¶ Drawing from his access to Snowden and his leaked documents, Greenwald describes Canada on the top tier of co-operation with the NSA, along with Australia, New Zealand and the United Kingdom.

## THE NSA BRIBES CANADA FOR ASSISTANCE IN SURVEILLANCE.

Peter Edwards, [Star Reporter], "Canada actively spies for NSA, Glenn Greenwald claims in new book," The Star, <http://www.thestar.com/news/canada/2014/05/13/canada_actively_spies_for_nsa_new_book_say> s.html, May 13, 2014.

He writes that “the NSA often maintains these partnerships by paying its partner to develop certain technologies and engage in surveillance, and can thus direct how the spying is carried out. The Fiscal Year 2012 ‘Foreign Partner Review’ reveals numerous countries that have received such payment, including Canada, Israel, Japan, Jordan, Pakistan, Taiwan and Thailand.”

In 2012, Canada took at least $325,000 in research money, placing it fourth among co-operating countries, behind Pakistan, Jordan and Ethiopia, Greenwald writes.

## NSA SURVEILLANCE VIOLATES CIVIL LIBERTIES.

Peter M. Shane, [Chair in Law, Moritz College of Law, Ohio State University], "Foreword: The NSA And the Legal Regime for Foreign Intelligence Surveillance," A Journal of Law and Policy for the Information Society, 2014.

For civil libertarians, however, any such argument is quite likely to pale given the more ¶ direct civil liberties impacts of mass surveillance. In NSA Surveillance: The Implications for ¶ Civil Liberties, Shayana Kadidal, the senior managing attorney of the Guantánamo Global ¶ Justice Initiative at the Center for Constitutional Rights in New York City, asserts that such ¶ programs threaten the very independence of citizen thought and action that are central to ¶ democratic governance.144 He illustrates that idea concretely by explaining the impact of the ¶ NSA programs on his own work and on the work of other lawyers who represent politically ¶ unpopular or vulnerable clients. Like Professors Mueller and Stewart, he also calls into question ¶ the “liberty-security tradeoff” meme. Like them, he calls into question the few successes ¶ publicly identified with the NSA programs and worries, as they do, that the extraordinary rate of ¶ false positives means that the FBI is too often spending significant time and effort on leads that ¶ go nowhere.145

## THERE ARE FOUR WAYS THAT DIGITAL SURVILLANCE VIOLATES PRIVACY.

Nikki Gulzar et al, [Auckland University of Technology], "Surveillance Privacy Protection," [http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf,](http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf) 2013.

Phishing may be used for private information. How this is done is that usually cybercriminals send emails or maybe instant messages that look like they are from trusted organization and may require personal information or mobile num-¶ Surveillance Privacy Protection 87¶ bers. Someone who is not familiar with technology and the risks that come with handing out personal information may fall for one of these traps. It is important to educate family, friends, and colleagues about the risks of disclosing sensitive information. When it comes to personal information, we should always provide bare minimum.¶ • Using malware and spyware has become quite common when extracting personal information. Today cyber criminals just use malicious web sites to download pro- grams through security holes in software on the PCs [96]. Anti-virus is important for protecting PCs, especially in today’s digital world, where most of our personal data are stored electronically.¶ • Storing data electronically has become very popular. With electronically stored data, risk of privacy breach has increased. Law has been tightened for medical storage, however there are still some loopholes that have been identified. It is important to talk to companies and organizations about privacy concerns and un- derstand how our data is being protected.¶ • Wireless hotspots are just about everywhere around the globe. Public Wi-Fi con- nection can make it easy for hackers to gain access. It is important to have a strong and operating firewall and avoid entering financial information because the data that is being carried over the public Wi- Fi networks may not be encrypted [96].

## LIBERAL DEMOCRACY DEMANDS THE RIGHT TO PRIVACY.

David Cole, [Georgetown University Law Center], "Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism," in Surveillance, Counter-Terrorism, and Comparative Constitutionalism, New York: Routledge 2013.

In 1956, at the height of McCarthyism in the US, sociologist Edward Shils¶ wrote that liberal democracy demands confidentiality for its citizens and¶ transparency foritsgovernment.8 Today, it is the citizenry that is increasingly¶ transparent, while government operations are shrouded in secrecy. That¶ development poses a serious challenge not merely to privacy but to liberty¶ and democracy. Sir Thomas Erskine May's words from 1863 apply with¶ equal if not greater immediacy 150 years later:¶ Next in importance to personal freedom is immunity from suspicions¶ and jealous observation. Men may be without restraints upon their liberty; they may pass to and fro at pleasure; but if their steps are tracked¶ by spies and informers, their words noted down for crimination, their¶ associates watched as conspirators - who shall say that they are free?¶ Nothing is more revolting to Englishmen than the espionage which¶ forms part of the administrative system of continental despotisms. It¶ haunts men like an evil genius, chills their gaiety, restrains their wit, casts¶ a shadow over their friendships, and blights their domestic hearth. The¶ freedom of this country may be measured by its immunity from this¶ baleful agency.9

## NSA PROGRAMS ARE OUTRAGEOUSLY EXPENSIVE.

John Mueller [political scientist at Ohio state] and Mark G. Stewart [civil engineer at the University of Newcastle in Australia], "Three Questions about NSA Surveillance," Cato Institute, June 13, 2013.

After 9/11, U.S. intelligence concluded that there were thousands of Al Qaeda operatives in the country. That perspective impelled a vast and hasty increase in spending on intelligence and policing, and at least 263 military and intelligence agencies have been created or reorganized. For its part, the Department of Homeland Security has set up a vast array of “fusion centers” to police terrorism, but is unable to determine how much they cost. It estimates that somewhere between $289-million and $1.4-billion were awarded to them from 2003 to 2010—a gap of over a billion dollars that is impressive even by Washington standards.

## THE NUMBER OF AL QAEDA OPERATIVES IN THE US DOES NOT JUSTIFY THE DOLLARS SPENT ON SURVEILLANCE.

John Mueller [political scientist at Ohio state] and Mark G. Stewart [civil engineer at the University of Newcastle in Australia], "Three Questions about NSA Surveillance," Cato Institute, June 13, 2013.

As it turned out, the number of Al Qaeda operatives actually in the United States registered at zero or nearly so, and the threat of terrorism in the country proved to be far more limited than initially feared. Accordingly, there might logically have been some judicious cutbacks in the funds devoted to the expensive quest to find terrorists who mostly didn’t exist—a process some in the FBI call “ghost chasing.”¶ However, the reaction has continually been to expand the enterprise, searching for the needle by adding more and more hay. Far overdue are extensive openly published studies that rationally evaluate homeland-security expenditures.¶ The NSA’s formerly secret surveillance programs have been part of the expansionary process. If they have done little to prevent terrorist attacks in the United States, and if we are now having what President Obama has characterized as a “healthy” debate about the programs, it seems reasonable to suggest that the debaters should at least be supplied with information about how much the programs cost.

*DEMOCRATIC FREEDOMS*

## Page 122 of 176

## SURVEILLANCE HAS A CHILLING EFFECT ON ALL DEMOCRATIC FREEDOMS

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Privacy Is Worth Protecting," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-> imagined

These abuses are real, but if we focus on them exclusively we risk overlooking the deeper implications of pervasive government surveillance. When people think the government is watching them, or that it might be, they become reluctant to exercise democratic freedoms. They may be discouraged from visiting officially disfavored Web sites, joining controversial political groups, attending political rallies or criticizing government policy. This is a cost to the people who don’t exercise their rights, but it’s a cost to our society, too. The chilling effect of surveillance makes our public debates narrower and more inhibited and our democracy less vital. This is the greater threat presented by the kinds of programs that were exposed this past week.

## SURVEILLANCE CREATES A CULTURE OF FEAR AND DISTRUST

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Democracy Requires Public Accountability," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-> threat-real-or-imagined

Eric, on your last point about the existence or nonexistence of a chilling effect, let me just point you to this recent report about the effect that surveillance by the New York Police Department has had on the Muslim community in and around New York City. The report concludes that “surveillance of Muslims’ quotidian activities has created a pervasive climate of fear and

suspicion, encroaching upon every aspect of individual and community life.” I wasn’t surprised by this conclusion. In the 1970s, the Church Committee came to similar conclusions about the effect that government surveillance had had on the political engagement of African-Americans. Your claim about the pervasiveness and banality of government secrecy elides the fact that there are many kinds of secrecy. Not all of them present the same threat to democracy. I don’t think our democracy is made weaker by the government’s withholding of information about the technical means it uses to effect surveillance. I don’t think our democracy is made weaker by the government’s withholding of information about the specific targets of its surveillance — so long as the surveillance is in fact limited to specific targets and so long as there is some mechanism that permits the public to evaluate the government’s conduct after the investigation is complete.

Secrecy about government policy, though, seems to me a very different thing. The whole point of democracy is to make government accountable to the public. How can the public hold government accountable if it doesn’t know what the government’s policies are? How can the public lobby Congress to amend the Patriot Act if it has no idea how the government has interpreted it? This is why I think that you have it backward when you say that “objections to the secrecy of the N.S.A. program are thus really objections to our political system itself.” It’s objections to transparency about the N.S.A. program that have this character. The argument that the government shouldn’t be required to tell the public what its policies are is an argument that we shouldn’t have a democracy.

## SURVEILLANCE DESTROYS ACCOUNTABLE DEMOCRACY AND PRIVACY

Auslin, Michael. [resident scholar and the director of Japan Studies at the American Enterprise Institute]. "Big Brother and the end to freedom," American Enterprise Institute. August 23, 2013,<http://aei.org/article/politics-and-public-opinion/big-brother-and-the-end-to-freedom/>

A great piece by David Rieff in Foreign Policy on Thursday discusses ”why nobody cares about the surveillance state.” The take away Big Question comes in the last two paragraphs: It is important to be clear. Does the public take the revelations of the data-mining scandal as an affront to their liberty? Presumably many, perhaps even most, do. But life is so full of affronts about which one would be an utter fool to imagine that one can do anything. The automated recordings through which one so often has to pay one’s bills, arrange an appointment, or try to get information (even whom to speak with to get that information) are an affront. The endless passwords, PINs, and the like are an affront (and are also, by definition, recorded on corporate databases). The ubiquitous CCTV cameras in city centers, a great many of which were installed well before the Sept. 11 attacks as crime-prevention and traffic-control measures, are an affront. And of course, all the petty and not so petty inconveniences and impositions of the post-9/11 world — from the preposterous demand that one show ID when entering not just a government building but almost any office building in America, to the shameless slovenliness and rudeness of Transportation Security Administration employees at every U.S. airport — are flagrant affronts.

Even if the long war against the jihadis were to end tomorrow with total victory for the United States, can anyone seriously suggest that any of these measures would be lessened, let alone canceled? The great myth of the past 25 years may be empowerment through technology. But the great truth of the past 25 years has been the rise of the surveillance state, which grows stronger every day — both because of technology itself and because of the control that states and huge corporations have over the technology that people depend upon and love. On one level, everyone knows this, but whether it’s because they believe themselves to be immune or because they simply never imagined that the surveillance state had become so all- encompassing, the elites seem to have been particularly surprised and therefore indignant over the scope of the NSA’s spying, the ardor with which governments have defended these practices, and their foaming rage at having to defend them in public at all. “This is the way the world ends,”

T. S. Eliot famously wrote in his great poem The Hollow Men, “not with a bang but a whimper.” Welcome to the post-democratic world. Oh, and by the way, you’ve been living in it for quite some time now. Rieff is on to the opiate-of-the-masses question, and it has already been answered in the affirmative. What governments don’t yet seem to get (or care about) is the self-inflicted wounds they are making, cultivating huge and growing resevoirs of distrust and cynicism. Society as a whole is being infected and governance will become ever more fraught thanks to the overreach, arrogance, and lack of self-control on the part of elites. As always, liberty will have to find the hidden nooks and crannies through which to flow, slowly wearing down the rocks of state power and control.

## NSA SURVEILLANCE IS THE DEATH KNELL FOR DEMOCRACY

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," 126 Harvard Law Review. 1904 (2013), <http://www.harvardlawreview.org/media/pdf/vol126_cohen.pdf>

If, as I have argued, the capacity for critical subjectivity shrinks in conditions of diminished privacy, what happens to the capacity for democratic self-government? Conditions of diminished privacy shrink the latter capacity as well, because they impair the practice of citizenship. But a liberal democratic society cannot sustain itself without citizens who possess the capacity for democratic self-government. A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy. Under such conditions, liberal democracy as a form of government is replaced, gradually but surely, by a different form of government that I will call modulated democracy because it relies on a form of surveillance that operates by modulation. Modulation and modulated democracy are emerging as networked surveillance technologies take root within democratic societies characterized by advanced systems of informational capitalism. Citizens within modulated democracies — citizens who are subject to pervasively distributed surveillance and modulation by powerful commercial and political interests — increasingly will lack the ability to form and pursue meaningful agendas for human flourishing.

## OPEN, FREE TECHNOLOGY IS NECESSARY TO BE AN ENGAGED CITIZEN

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," 126 Harvard Law Review. 1904 (2013), <http://www.harvardlawreview.org/media/pdf/vol126_cohen.pdf>

Networked information technologies mediate our experiences of the world in ways directly related to both the practice of citizenship and the capacity for citizenship, and so they configure citizens as directly or even more directly than institutions do. The practice of citizenship requires access to information and to the various communities in which citizens claim membership. In the networked information society, those experiences are mediated by search engines, social networking platforms, and content formats. Search engines filter and rank search results, tailoring both the results and the accompanying advertising to what is known about the searcher and prioritizing results in ways that reflect popularity and advertising payments. Social networking platforms filter and systematize social and professional relationships according to their own logics. Content formats determine the material conditions of access to information — for example, whether a video file can be copied or manipulated, or whether a news forum permits reader comments. Each set of processes structures the practice of citizenship and also subtly molds network users’ understanding of the surrounding world.27 To an increasing degree, then, the capacity for democratic self-government is defined in part by what those technologies and other widely used technologies allow, and by exactly how they allow it.

## SURVEILLANCE STIFLES INDIVIDUAL INNOVATION AND FREE THOUGHT

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," 126 Harvard Law Review. 1904 (2013), <http://www.harvardlawreview.org/media/pdf/vol126_cohen.pdf>

Conditions of diminished privacy also impair the capacity to innovate. This is so both because innovation requires the capacity for critical perspective on one’s environment and because innovation is not only about independence of mind. Innovation also requires room to tinker, and therefore thrives most fully in an environment that values and preserves spaces for tinkering. A society that permits the unchecked ascendancy of surveillance infrastructures, which dampen and modulate behavioral variability, cannot hope to maintain a vibrant tradition of cultural and technical innovation. Efforts to repackage pervasive surveillance as innovation — under the moniker “Big Data” — are better understood as efforts to enshrine the methods and values of the modulated society at the heart of our system of knowledge production. The techniques of Big Data have important contributions to make to the scientific enterprise and to social welfare, but as engines of truth production about human subjects they deserve a long, hard second look.

## SURVEILLANCE CONSTRAINS FREEDOM OF INNOVATION AND EXPERIMENTATION

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," Harvard Law Review. vol. 126, pg. 1904 (2013),<http://www.harvardlawreview.org/media/pdf/vol126_cohen.pdf>

When the predicate conditions for innovation are described in this way, the problem with characterizing privacy as anti-innovation becomes clear: it is modulation, not privacy, that poses the greater threat to innovative practice. Regimes of pervasively distributed surveillance and modulation seek to mold individual preferences and behavior in ways that reduce the serendipity and the freedom to tinker on which innovation thrives. The suggestion that innovative activity will persist unchilled under conditions of pervasively distributed surveillance is simply silly; it derives rhetorical force from the cultural construct of the liberal subject, who can separate the act of creation from the fact of surveillance. As we have seen, though, that is an unsustainable fiction. The real, socially constructed subject responds to surveillance quite differently — which is, of course, exactly why government and commercial entities engage in it. Clearing the way for innovation requires clearing the way for innovative practice by real people. Innovative practice in turn requires breathing room for critical selfdetermination and physical spaces within which the everyday practice of tinkering can thrive.

## SURVEILLANCE UNDERMINES RIGHTS TO FREE SPEECH AND PRIVACY

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013),<http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf>

Intellectual-privacy theory explains why we should extend chillingeffect protections to intellectual surveillance, especially traditional-style surveillance by the state. If we care about the development of eccentric individuality and freedom of thought as First Amendment values, then we should be especially wary of surveillance of activities through which those aspects of the self are constructed.90 Professor Timothy Macklem argues that “[t]he isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and the subversive.”91 A meaningful measure of intellectual privacy should be erected to shield these activities from the normalizing gaze of surveillance. This shield should be justified on the basis of our cultural intuitions and empirical insights about the normalizing effects of surveillance. But it must also be tempered by the chilling- effect doctrine’s normative commitment to err on the side of First Amendment values even if proof is imperfect.

## SURVEILLANCE INEVITABLY DETERS TRULY FREE SPEECH

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013),<http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf>

The mechanics of intellectual privacy discussed so far depend upon knowing, or at least fearing, that someone might be watching us. If we have a sense of privacy, even one that turns out to be an illusion, we are less likely to change our behavior under the panoptic gaze. Truly secret and unexpected surveillance, from this perspective, might appear not to violate our intellectual privacy at all. If we have no inkling that we are being watched, if we really do not care that we are being watched, or if we fear no consequences of being watched, it could be argued that our intellectual freedom is unaffected. It can thus be argued that if the NSA Wiretapping Program had never leaked, it would have posed no threat to intellectual privacy. There are two problems with this account. First, no program of widespread surveillance is likely to remain secret forever. At some point, such a program will inevitably come to light, either by being leaked (as happened with the NSA program and the Army surveillance in Laird), or by actions taken pursuant to the program (such as prosecutions or disclosures). The injury suffered by those thus punished would serve as an example to the rest of us, and the mechanisms of intellectual privacy would come into effect at that point.

*IMMIGRATION*

## VIOLATION OF DIGITAL PRIVACY CAN LEAD TO WRONGFUL DETAINMENT.

Anil Kalhan, [Associate Professor of Law, Drexel University], "Immigration Policing and Federalism Through the Lens of Technology, Surveillance, and Privacy," Ohio State Law Journal, 2013.

In short, the combination of database errors, automation bias, complex but ¶ time-pressured decisionmaking, massive volumes of inquiries, and fragmented ¶ responsibilities among different immigration agencies can easily yield ¶ circumstances in which immigration agencies rush to issue detainers first, and ¶ ask questions either later or never.146 Closer empirical research on immigration ¶ agency enforcement processes certainly would help illuminate whether that is, ¶ in fact, a fair characterization of the outcomes that Secure Communities ¶ produces, and while the program has contributed to a tenfold increase in the ¶ number of ICE detainers, recently issued guidelines for issuing detainers may ¶ shift these outcomes.147 Nevertheless, at least under recent practices, the limited ¶ exercise of discretion by immigration officials at the prosecution and ¶ adjudication stages of the removal process makes the moment of arrest ¶ critical—the “discretion that matters,” as Hiroshi Motomura explains—in ¶ affecting whether an individual ultimately is removed.148 Especially given the ¶ limited procedural protections and access to counsel afforded to noncitizens ¶ facing removal proceedings, particularly for individuals in detention, the ¶ consequences of database errors and other fallibilities of automation at the ¶ initial stages of the removal process can be difficult to correct and remedy once ¶ the agency has acted upon them.149

## NSA SURVEILLANCE DISPROPORTIONATELY AFFECTS IMMIGRANTS

Conor Friedersdorf, “NSA Spying Has a Disproportionate Effect on Immigrants,” *The Atlantic* (Online), May 16, 2014. URL = <<http://www.theatlantic.com/politics/archive/2014/05/nsa-spying-> has-a-disparate-impact-on-the-privacy-rights-of-us-immigrants/371023/>

All I'd add is that the Obama administration's encroachments on the Fourth Amendment disparately affect naturalized citizens of the United States, almost all of whom still have friends or family members living in their countries of origin. When I call my parents, email my sister, or text my best friend, my private communications are theoretically protected by the Bill of Rights. In contrast, immigrants contacting loved ones often do so with the expectation that every word they say or write can be legally recorded and stored forever on a server somewhere.

Xenophobia is one factor driving this double-standard. It does real harm to immigrants whose speech is chilled, as is clear to anyone who has made an effort to speak with them.

Yet there has been little backlash against the Obama administration for affording zero constitutional protections to Americans engaged in speech with foreigners, and little sympathy for the innocent Americans, many of them immigrants, who are hurt by the approach Obama and many in Congress endorse.

## NSA SURVEILLANCE VIOLATES THE CONSTITUTION.

Peter M. Shane, [Chair in Law, Moritz College of Law, Ohio State University], "Foreword: The NSA And the Legal Regime for Foreign Intelligence Surveillance," A Journal of Law and Policy for the Information Society, 2014.

Professors Katherine Strandberg and Laura Donahue argue, however, that the programs ¶ Snowden revealed violate constitutional rights protections in other respects. In Membership ¶ Lists, Metadata, and Freedom of Association’s Specificity Requirement,¶ 138 Professor Strandberg ¶ argues that metadata surveillance is unconstitutional unless conducted in compliance with the ¶ First Amendment’s guarantee of freedom of association. As analyzed by Professor Strandburg, ¶ that right entails certain specificity requirements that the current Section 215 programs do not ¶ meet. In PRISM and the Interception of Communications Under Section 702 of the Foreign ¶ Intelligence Surveillance Act,¶ 139 Professor Laura Donohue argues, Smith notwithstanding, the ¶ NSA’s Internet content surveillance program fails Fourth Amendment requirements. She agrees ¶ with Professor Yoo that the program is consistent with FISA, but argues that the program is ¶ unconstitutional because of the compulsory involvement of private telecom companies and the failure to prevent overbreadth. She concludes that the interception of all international ¶ communications fails the reasonableness test of Katz.

## THE US SUPREME COURT HAS RULED AGAINST VIOLATIONS OF PRIVACY ON THE FOURTH AMENDMENT

David Cole, [Georgetown University Law Center], "Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism," in Surveillance, Counter-Terrorism, and Comparative Constitutionalism, New York: Routledge 2013.

In 2012, the US Supreme Court (USSCt) issued what could be one of its¶ most important privacy decisions in decades, as it took up one version of this¶ issue -¶ namely, whether police use of a global positioning system (GPS)¶ device to monitor the public movements of a car for a month amounted to a¶ search subject to constitutional constraints. The case of United States v Jones¶

{Jones) generated a¶ surprising unanimous decision concluding that the prohibition on unreasonable searches in the Fourth Amendment to the US¶ Constitution was implicated, but the justices were sharply divided in their¶ reasoning.5 Some justices looked back to notions of property to find that the¶ police action was a search; others looked forward, warning that technology¶ enables the police to invade privacy in ways unheard of when the Fourth¶ Amendment was adopted. That division of reasoning and outlook is emblematic of the uncertainty that new technology has created for the constitutional¶ law of privacy.

## NSA SURVEILLANCE IS ILLEGAL

Sanchez, Julian. [research fellow at the Cato Institute]. "NSA Surveillance Violated Constitution, Secret FISA Court Found," The CATO Institute. July 23, 2012, <http://www.cato.org/blog/nsa-> surveillance-violated-constitution-secret-fisa-court-found

Americans are being told that there’s no need to worry about the broad surveillance programs authorized by the controversial FISA Amendments Act of 2008. Yet a report from Wired this weekend paints a more disturbing picture: National Security Agency surveillance enabled by the FAA was found “unreasonable under the Fourth Amendment” by the secretive Foreign Intelligence Surveillance Court “on at least one occasion.” The court also found that the government’s implementation of its authority under the statute had “circumvented the spirit of the law.” Despite these troubling rulings from a court notorious for its deference to intelligence agencies, Congress is so unconcerned that lawmakers don’t even want to know how many citizens have been caught up in the NSA’s vast and growing databases.

## NSA SURVEILLANCE VIOLATES THE FOURTH AMENDMENT

Sanchez, Julian. [research fellow at the Cato Institute]. "NSA Surveillance Violated Constitution, Secret FISA Court Found," The CATO Institute. July 23, 2012, <http://www.cato.org/blog/nsa-> surveillance-violated-constitution-secret-fisa-court-found

That first statement is almost certainly a direct reference to Sen. Dianne Feinstein’s assertions in a recent report from the Senate Intelligence Committee—which noted that the Court has blessed much of the surveillance under Section 702, the part of the FAA that permits warrantless acquisition of international communications. Given the massive volume of NSA surveillance, however, the fact that some NSA surveillance was held constitutional is much less significant, for purposes of public accountability, than the fact that some of it was unconstitutional. Feinstein’s summary of those positive classified opinions was made public weeks ago, apparently without much trouble. Yet only now that the FAA renewal has made it through multiple committees is the public permitted to know—after much tooth-pulling from a senator, via a letter released late on a Friday afternoon—how incomplete that summary really was. It’s cause for concern any time government exceeds the bounds of the Fourth Amendment, but it should be truly worrying when it’s in the context of mass-scale spying by the NSA. Based on what little we know of the NSA’s programs from public reports, a single “authorization” will routinely cover hundreds or thousands of phone numbers and e-mail addresses. That means that even if there’s only “one occasion” on which the NSA “circumvented the spirit of the law” or flouted the Fourth Amendment, the rights of thousands of Americans could easily have been violated.

## NSA SURVEILLANCE IS AN UNACCEPTABLE INFRINGEMENT OF THE 4TH AMENDMENT

Sanchez, Julian. [research fellow at the Cato Institute]. "NSA Surveillance Violated Constitution, Secret FISA Court Found," The CATO Institute. July 23, 2012, <http://www.cato.org/blog/nsa-> surveillance-violated-constitution-secret-fisa-court-found

Binney argues that when NSA officials have denied they are engaged in broad and indiscriminate “interception” of Americans’ communications, they are using that term “in a very narrow way,” analogous to the technical definition of “collection” above, not counting an e-mail or call as “intercepted” until it has been reviewed by human eyes. On this theory, the entire burden of satisfying the Fourth Amendment’s requirement of “reasonableness” is borne by the “minimization procedures” governing the use of the massive Pinwale database. On this theory, the

constitutional “search” does not occur when all these billions of calls and emails are actually intercepted (in the ordinary sense) and recorded by the NSA, but only when the database is queried. This is a huge departure from what has traditionally been understood to be constitutionally permitted. We do not normally allow the government to indiscriminately make copies of everyone’s private correspondence, so long as they promise not to read it without a warrant: The copying itself is supposed to require a warrant, except in extraordinary circumstances. It appears almost certain that a very different rule is in effect now, at least for the NSA. It cannot be overemphasized how dangerous such a change would be. Traditionally, a citizen’s right to private communication was either respected or violated at the time it occurred: Your rights would be violated in realtime, or not at all, and even in the lawless era of J. Edgar Hoover, only so many citizens could be spied on at once. Under this new regime, the threat to our rights is perpetual. Even if this administration and the next are scrupulous about respecting civil liberties, even if every man and woman currently employed by the NSA is noble and pure of heart, the conversation you have today may well be there for the use or misuse of whoever holds power in ten years, or fifteen, or twenty. Will the incumbent president in 2032 resist the temptation to hunt for dirt in online chats from his opponent’s college years—showing greater restraint than so many past presidents? One must hope so—but better to design the rules of a free society so that such leaps of faith aren’t required.

## SURVEILLANCE VIOLATES CONSTITUTIONAL GUARANTEES OF INTELLECTUAL FREEDOM

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013),<http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf>

Shadowy regimes of surveillance corrode the constitutional commitment to intellectual freedom that lies at the heart of most theories of political freedom in a democracy. Secret programs of wide-ranging intellectual surveillance that are devoid of public process and that cannot be justified in court are inconsistent with this commitment and illegitimate in a free society. My argument is not that intellectual surveillance should never be possible, but that when the state seeks to learn what people are reading, thinking, and saying privately, such scrutiny is a serious threat to civil liberties. Accordingly, meaningful legal process (that is, at least a warrant supported by probable cause) must be followed before the government can perform the digital equivalent of reading our diaries. But we must also remember that in modern societies, surveillance fails to respect the line between public and private actors. Intellectual privacy should be preserved against private actors as well as against the state. Federal prosecutions based on purely intellectual surveillance are thankfully rare, but the coercive effects of monitoring by our friends and acquaintances are much more common. We are constrained in our actions by peer pressure at least as much as by the state. Moreover, records collected by private parties can be sold to or subpoenaed by the government, which (as noted above) has shown a voracious interest in all kinds of personal information, particularly records related to the operation of the mind and political beliefs.95 Put simply, the problem of intellectual privacy transcends the public/private divide, and justifies additional legal protections on intellectual privacy and the right to read freely.96 Constitutional law and standing doctrine alone will not solve the threat of surveillance to intellectual freedom and privacy, but they are a good place to start.

## THE SURVEILLANCE AUTHORITY CLAIMED BY THE NSA IS SWEEPING AND OVERBROAD

Conor Friedersdorf, “NSA Spying Has a Disproportionate Effect on Immigrants,” *The Atlantic* (Online), May 16, 2014. URL = <<http://www.theatlantic.com/politics/archive/2014/05/nsa-spying-> has-a-disparate-impact-on-the-privacy-rights-of-us-immigrants/371023/>

The U.S. government concedes that it needs a warrant to eavesdrop on phone calls between Americans, or to read the body of their emails to one another. Everyone agrees that these communications are protected by the Fourth Amendment. But the government also argues that Fourth Amendment protections don't apply when an American calls or writes to a foreigner in another country.

Let's say, for example, that the head of the NAACP writes an email to a veteran of the South African civil-rights struggle asking for advice about an anti-racism campaign; or that Hillary Clinton fields a call from a friend in Australia whose daughter was raped; or that Jeb Bush uses Skype to discuss with David Cameron whether he should seek the 2016 presidential nomination for the Republican Party. Under the Obama administration's logic, these Americans have no reasonable expectation of privacy with regard to these conversations, and it is lawful and legitimate for the NSA to eavesdrop on, record, and store everything that is said.

The arguments Team Obama uses to justify these conclusions are sweeping and worrisome, as the ACLU's Jameel Jaffer captures in his analysis of the relevant legal briefs:

... the government contends that Americans who make phone calls or send emails to people abroad have a diminished expectation of privacy because the people with whom they are communicating—non-Americans abroad, that is—are not protected by the Constitution. The government also argues that Americans' privacy rights are further diminished in this context because the NSA has a "paramount" interest in examining information that crosses international borders.

... the government even argues that Americans can't reasonably expect that their international communications will be private from the NSA when the intelligence services of so many other countries ... might be monitoring those communications, too. The government's argument is not simply that the NSA has broad authority to monitor Americans' international communications. The US government is arguing that the NSA's authority is unlimited in this respect. If the government is right, nothing in the Constitution bars the NSA from monitoring a phone call between a journalist in New York City and his source in London. For that matter, nothing bars the NSA from monitoring every call and email between Americans in the United States and their non-American friends, relatives, and colleagues overseas.

## THE GOVERNMENT ARGUES THAT AMERICANS HAVE ESSENTIALLY NO REASONABLE EXPECTATION OF PRIVACY IN ELECTRONIC COMMUNICATIONS

Jameel Jaffer, “The official US position on the NSA is still unlimited eavesdropping power,”

*Guardian* (Online), May 14th, 2014. URL =

<<http://www.theguardian.com/commentisfree/2014/may/14/nsa-eavesdropping-program-> constitutional>

Modern American privacy law begins with Charles Katz, an accused gambler, making a call from a Los Angeles phone booth. In a now-famous opinion, Justice John Marshall Harlan concluded that the US Constitution protected Katz's "expectation of privacy" in his call. American phone booths are now a thing of the past, of course, and Americans' expectations of privacy seem to be fast disappearing, too. ¶ In two significant but almost-completely overlooked legal briefs filed last week, the US government defended the constitutionality of the Fisa Amendments Act, the controversial 2008 law that codified the Bush administration's warrantless-wiretapping program. That law permits the government to monitor Americans' international communications without first obtaining individualized court orders or establishing any suspicion of wrongdoing. ¶ It's hardly surprising that the government believes the 2008 law is constitutional – government officials advocated for its passage six years ago, and they have been vigorously defending the law ever since. Documents made public over the last eleven-and-a-half months by the Guardian and others show that the NSA has been using the law aggressively. ¶ What's surprising – even remarkable – is what the government says on the way to its conclusion. It says, in essence, that the Constitution is utterly indifferent to the NSA's large-scale surveillance of Americans' international telephone calls and emails:

The privacy rights of US persons in international communications are significantly diminished, if not completely eliminated, when those communications have been transmitted to or obtained from non-US persons located outside the United States.

That phrase – "if not completely eliminated" – is unusually revealing. Think of it as the Justice Department's twin to the NSA's "collect it all".¶ The government filed the legal briefs last week in two criminal cases, one in Colorado and another in Oregon, in which the defendants are being prosecuted based on evidence acquired under the Fisa Amendments Act. Both defendants have sought to have the government's evidence suppressed on the grounds that the surveillance law is unconstitutional. (The ACLU joined with the defense team in the Colorado case to make that argument.) ¶ In support of the law, the government contends that Americans who make phone calls or send emails to people abroad have a diminished expectation of privacy because the people with whom they are communicating – non-Americans abroad, that is – are not protected by the Constitution. ¶ The government also argues that Americans' privacy rights are further diminished in this context because the NSA has a "paramount" interest in examining information that crosses international borders. ¶ And, apparently contemplating a kind of race to the bottom in global privacy rights, the government even argues that Americans can't reasonably expect that their international communications will be private from the NSA when the intelligence services of so many other countries – the government doesn't name them – might be monitoring those communications, too. ¶ The government's argument is not simply that the NSA has broad authority to monitor Americans' international communications. The US government is arguing that the NSA's authority is unlimited in this respect. If the government is right, nothing in the Constitution bars the NSA from monitoring a phone call between a journalist in New York City and his source in London. For that matter, nothing bars the NSA from monitoring every call and email between Americans in the United States and their non-American friends, relatives, and colleagues overseas. ¶ In the government's view, there is no need to ask whether the 2008 law violates Americans' privacy rights, because in this context Americans have no rights to be violated.

## THE HOUSE RECENTLY PASSED A BILL TO LIMIT NSA SURVEILLANCE.

Eileen Sullivan, [Associated Press], "House Committees Pass BIll on NSA Surveillance," ABC News, [http://abcnews.go.com/Politics/wireStory/house-committees-pass-bill-nsa-surveillance-](http://abcnews.go.com/Politics/wireStory/house-committees-pass-bill-nsa-surveillance-23643354)  [23643354,](http://abcnews.go.com/Politics/wireStory/house-committees-pass-bill-nsa-surveillance-23643354) May 8, 2014.

The House crossed a major hurdle in its efforts to rein in the National Security Agency when two oversight committees agreed this week on a proposal to end the agency's practice of collecting Americans' phone records and the bulk collection of all other records, such as credit card data. The House could vote on the bill as early as this month.¶ It was the first sign of consensus in the bitterly divided House on the controversial NSA surveillance programs since the spying was disclosed nearly a year ago. President Barack Obama has called for similar changes but is relying on Congress to hammer out the details. Senate oversight committees have yet to agree, which would be necessary before any new law is approved.¶ The House proposal — passed Wednesday by the Judiciary Committee and Thursday by the Intelligence Committee — would strengthen privacy safeguards for Americans' communications that are swept up by the NSA. It also would require more transparency for disclosing how often private companies cooperate with the government on records requests.¶ Obama has not formally backed any of the proposals under consideration, but a White House spokeswoman said the bill is a "very good step."¶

## NEW ATTEMPTS TO REGULATE NSA SURVEILLANCE ARE BEING WATERED DOWN

Siobhan Gorman, “Privacy Groups Back Away From NSA Bill Over Changes,” *Wall Street Journal*

(Online), May 20th, 2014. URL =

<<http://online.wsj.com/news/articles/SB10001424052702304422704579574513519775336>>

The amended bill released Tuesday by House leaders is still expected to pass the chamber later this week. But a sudden revolt by privacy advocates suggests the floor debate likely will be more contentious.

The issue centers on the definition of the term used to describe the search terms for phone databases or other large data sets, called a "selector."

Earlier versions of the bill limited search terms to "a person, account, or entity." The new version of the bill says those three types of terms are just examples of what could be used, by inserting the language "such as" before the list.

The language now reads: "such as a term specifically identifying a person, entity, account, address, or device."

Privacy advocates say changes in the terms used to define the scope of an NSA search allow for broader data collection than earlier versions of the legislation and that the new bill is murkier on prohibiting mass collection of data.

People familiar with the negotiations said the changes were sought by intelligence officials.

"The bill has been gutted," said Harley Geiger, senior counsel at the Center for Democracy and Technology, a civil liberties advocacy group.

## THE USA FREEDOM ACT WILL INCLUDE NEW RESTRICTIONS ON NSA DATA STORAGE

Spencer Ackerman, “Restrictions placed on NSA's data store after intense talks over surveillance bill,” *Guardian* (Online), May 20th, 2014. URL =

<<http://www.theguardian.com/world/2014/may/20/nsa-reform-restrictions-data-surveillance-talks>>

Last-minute negotiations over the details of a congressional surveillance bill have resulted in

restrictions around the National Security Agency’s massive repository of analysed call data.

Intense closed-door talks between lawmakers and Obama administration and intelligence officials that wrapped up Tuesday afternoon have finalised the language of the USA Freedom Act. The bill is expected to receive a vote on the House floor on Thursday.

The latest twist for the bill is an expanded provision that would require the government to “promptly” purge phone records that do not contain “foreign intelligence information,” effectively pruning irrelevant records from the NSA’s trees of analyzed phone data.

Under the new provision, the government would have to “adopt minimisation procedures that require the prompt destruction of all call detail records” turned over by the telecoms firms “that the government determines are not foreign intelligence information.”

The government would ultimately have to “destroy all call detail records produced under the order as prescribed by such procedures”.

## THE USA FREEDOM ACT HAS GOTTEN WEAKER AND WEAKER OVER TIME

Spencer Ackerman, “Restrictions placed on NSA's data store after intense talks over surveillance

bill,” *Guardian* (Online), May 20th, 2014. URL =

<<http://www.theguardian.com/world/2014/may/20/nsa-reform-restrictions-data-surveillance-talks>>

Until now, the USA Freedom Act, increasingly the consensus bill for surveillance reforms, left the “corporate store” alone. ¶ Under the bill, the government would no longer collect call records in bulk. But it would be permitted to acquire Americans’ phone data when a judge certifies that there is reasonable articulable suspicion of a connection to terrorism or foreign espionage, and it can collect phone records from the contacts of the contacts – two “hops” – of the original person or phone account the government targets. ¶ The new language would apparently restrict the NSA from retaining data on the contacts of the targets not believed to have a connection to foreign intelligence information – what surveillance observers sometimes refer to as the “pizza guy” problem, where the NSA amasses data on random and irrelevant people or accounts connected to targets. ¶ But the language does not define key terms, such as how long a record can be withheld before its “prompt” destruction. Nor does it specify how the government will “determine”

a call record is unrelated to foreign intelligence information if, as can occur with the corporate store today, NSA’s automated programs sift through the data. ¶ "Placing meaningful limits on the NSA's use of this vast pool of data is crucial to protecting Americans' privacy – and to any reform effort. Congress should not leave the NSA with a wide open backdoor to many of Americans' call records via the corporate store,” said Patrick Toomey, a lawyer with the American Civil Liberties Union, who has focused on the corporate store. ¶ A deal on the corporate store restriction was easier to reach than over a different critical definition contained within the USA Freedom Act – one that defines the source of the records the government will be able to collect. ¶ That category is a “specific selection term.” That is the root data from which the government must suspect of connection to terrorism or espionage to launch the collection of call records. Without possessing that term, the government cannot collect obtain the call records at issue. ¶ The version of the USA Freedom Act that cleared House committees earlier this month defined it simply as a term that “uniquely describe[s] a person, entity, or account.” ¶ But the version that will head to the floor, at the Obama administration’s insistence, has broadened the definition, opening the door to broader data collection than the bill’s architect’s initially envisioned. ¶ The bill now defines a “specific selection term” as “a discrete term, such as a term specifically identifying a person,

entity, account, or device, used by the government to limit the scope of the information or tangible things sought.” ¶ Sources familiar with the process said the government had pushed for an even broader definition. ¶ Privacy groups had already watched with dismay as their favored bill gradually grew less restrictive on the NSA and its transparency requirements about what recipients of surveillance orders can disclose to their customers became weaker. ¶

## THE NSA COLLECTS DATA THROUGH PRIVATE TELECOMMUNICATIONS AND INTERNET SERVICE PROVIDERS.

David Cole, [Hon. George Mitchell professor in law and public policy at Georgetown University Law Center and is the legal affairs correspondent for the Nation.], "No Place to Hide by Glenn Greenwald, on the NSA's sweeping efforts to 'Know it All'," Washington Post, May 12, 2014.

The NSA achieves these ends by working hand in hand with private telecommunications and Internet service providers. One NSA document describes an unnamed corporate partner as “aggressively involved in shaping traffic to run signals of interest past our monitors” and reports that in a single month, this top-secret, public-private partnership yielded more than 6 billion records of telephone calls and Internet activity. Under another program revealed here, the NSA intercepts routers, servers and other network equipment being shipped overseas; installs back- door surveillance bugs; rewraps the packages with factory seals; and sends them on their way, thereby ensuring that the agency will have clandestine access to all information that passes through them.

## THE NSA CAN TRACK EVERY KEYSTROKE ON A COMPUTER.

David Cole, [Hon. George Mitchell professor in law and public policy at Georgetown University Law Center and is the legal affairs correspondent for the Nation.], "No Place to Hide by Glenn Greenwald, on the NSA's sweeping efforts to 'Know it All'," Washington Post, May 12, 2014.

Other documents describe X-KEYSCORE, the NSA’s most powerful tool, which, as its name implies, enables the agency to track every keystroke on a computer, permitting the agency to monitor in real time all of a user’s e-mail, social-media and Web-browsing activity. In a single month in 2012, X-KEYSCORE collected 41 billion records for one NSA unit. Greenwald contends that this is the program Snowden was referring to when he said that, with an e-mail address, he could tap into any American’s communications. (The NSA has accused Snowden of exaggerating, but the documents suggest that he may be right.)

## THERE ARE NUMEROUS TECHNIQUES TO BREACH DATABASE SECURITY.

Nikki Gulzar et al, [Auckland University of Technology], "Surveillance Privacy Protection," [http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf,](http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf) 2013.

Digital database technology is a pivot part of numerous computing systems. Data is permitted to be taken and distributed electronically and the level of data enclosed in these systems keeps rising at an exponential rate. That is why it is important to ensure the integrity of collected data and secure the private information from unauthorized access [42].¶ Technology such as smart phones is a great invention. It’s more practical than a laptop but what we don’t realize is that tracking someone’s mobile phone has be- come very easy with the help of applications that likes to use locations. Turning off those applications is only the first step in securing our mobile phone [29]. Usually, we store information on our mobile phones in case we don’t forget it. “Safe Note” is the application that allows personal information that we store on the phone to be encrypted using a pin. Also, all the “Safe Note” that are entered use a 128-bit en- cryption, which will make it difficult to get access to personal information stored on individual’s phone.¶ Another application that is used to encrypt and protect text and email messages is called encrypted messages. This application allows us to give a password to all the messages that we want to transmit and receive the message in encrypted form. If the message is intercepted, then the only way a person will be able to decrypt the message is whether they had the application and also knew the password that is used to encrypt the message [29]. Even having a conversation via a mobile phone is not safe, it is prone to interception. HeyTell VoIP application allows all data and audio in transit to be encrypted [29]. It is very easy to use, just set up the privacy level before we dial a number. It basically converts the mobile phones into a digital walkie-talkie with encrypted messages [29].

The only downfall of these applications is that the person we want to correspond with must have these applications installed on their phones, but with the popularity of smart phones nearly everyone has, thus this problem can be easily fixed.

## SURVEILLANCE IS A DIRECT ASSAULT ON PRIVACY.

Walter Simpson, [Contributor, Buffalo News], "The end of privacy? Government and private surveillance pose a growing threat to Americans," Buffalo News, May 10, 2013.

In contrast, surveillance is a direct assault on privacy. It attacks and eliminates privacy. Its chilling effect constrains and shrinks us through self-censorship of thought and action. When taken to the extreme, like in George Orwell’s “1984,” surveillance objectifies so thoroughly that it destroys our internal life.¶ Our nation’s founders recognized the importance of privacy in the Bill of Rights. The Fourth Amendment to the U.S. Constitution states, “The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated.”¶ While this language is pre-9/11, Internet and cellphone, it speaks of the kind of nation the founders envisioned. In America, we have a constitutionally guaranteed right to a private life safe from unreasonable search and seizure. But our privacy is being eroded by leaps and bounds every day.

## NSA ACTIONS ARE EGREGIOUS VIOLATIONS OF PRIVACY.

Walter Simpson, [Contributor, Buffalo News], "The end of privacy? Government and private surveillance pose a growing threat to Americans," Buffalo News, May 10, 2013.

As chronicled in Julia Angwin’s excellent book, “Dragnet Nation,” whenever we use our cellphones, tablets and computers, everything we do on them is tracked, recorded and stored by phone and Internet service providers. The apps we use and the websites we visit gather our personal data and use it to market products to us or sell it to third-party data brokers.¶ In fact, many Web providers invite third-party data-mining companies to spy on us, allowing them to secretly insert “cookies” and “Web beacons” onto our computers so they can track our activity as we go from website to website. Twenty or more of these undisclosed companies may be tracking us at any given time. The tracking data they gather is then used to create detailed personal profiles of Web users – each made up of as many as 1,000 data points, according to the Obama administration’s just-released “Big Data” report. These profiles are then marketed to other companies. This is how “free” websites and services make money.¶ Our personal communications, including online gaming activity, are also vacuumed up by the National Security Agency. Thanks to revelations by whistle-blower Edward Snowden, we know this U.S. spy agency employs a “collect it all” strategy when gathering information on our personal cellphone and online activities. Since 9/11, the NSA has used secret contracts with telecommunication giants and covert splicing into their communication cables to intercept Internet and cellphone information on hundreds of millions of Americans and foreigners who are not terrorist or criminal suspects. As pointed out by the American Civil Liberties Union and others, the NSA has not shown that this dragnet is effective in preventing terrorist activity.¶

## NSA SURVEILLANCE UNDERMINES OUR BASIC RIGHT TO PRIVACY

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Privacy Is Worth Protecting," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-> imagined

Well, Eric, we see this very differently. You think the privacy objection is “weak,” but the fact is that many people — I’d venture to say most — feel violated when their personal information is surreptitiously collected by the government. The complaint isn’t about “a general sense of creepiness.” The complaint is that a fundamental right — a right that society has traditionally protected and that society should protect — has been infringed. Of course we share personal information with government agents all the time. We share financial information with the I.R.S., we share information about our children with public school teachers, and so on. But the fact that we sometimes share discrete categories of information with specific categories of people for narrowly delineated purposes doesn’t seem to me to be very relevant. “Privacy” means being able to decide for ourselves whom our information is shared with, and when, and under what

conditions. Needless to say, the right of privacy shouldn’t trump everything. National security (and other government interests) may justify some narrow intrusions on privacy in some circumstances. The problem with the programs disclosed over last week is that they are so astonishingly broad.

## THE PROGRAM IS A MASSIVE INVASION OF PRIVACY

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Our Surveillance Laws Are Too Permissive," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-> threat-real-or-imagined

The Guardian revealed on Wednesday that the government has directed Verizon Business Network Services to hand over an array of sensitive information about every domestic and international phone call made by its customers in the United States over a three-month period. The directive, sanctioned by the secretive court that oversees government surveillance in some national security cases, requires Verizon to tell the government who made each call, whom they called, when they made the call, how long the call lasted, and (maybe) where the parties to the call were located. Reportedly, the N.S.A. has been serving all of the major telecommunications companies with similar “metadata” directives for at least seven years. Whatever else might be said about it, the program surely constitutes one of the most ambitious surveillance efforts ever undertaken by a democratic government against its own citizens. As if that weren’t enough, The Guardian and The Washington Post also revealed last week that the N.S.A. has secured direct access to the major Internet companies’ central servers. There seems to be some confusion about precisely what the N.S.A. is doing with that access, but The Washington Post reports that the agency is collecting information about surveillance targets believed (with 51 percent certainty) to be outside the United States and about people one and two degrees removed from these targets. So the N.S.A. might focus initially on, say, a British journalist working at Der Spiegel, collecting all of her e-mail communications as well as all uploaded videos, photos, Web surfing data, social media posts — and then collect the same information about all of the contacts in the journalist’s address book and then about all of the contacts in their address books.

## MISTAKES THAT CAUSE ABUSE AND INVASIONS OF PRIVACY ARE INEVITABLE

Gerecht, Reuel. [senior fellow at the Foundation for Defense of Democracies and a former case officer in the CIA’s clandestine service]. "The Costs and Benefits of the NSA," The Weekly Standard. June 24, 2013, <http://www.weeklystandard.com/articles/costs-and-benefits-> nsa\_735246.html

Should Americans fear the possible abuse of the intercept power of the National Security Agency at Fort Meade, Maryland? Absolutely. In the midst of the unfolding scandal at the IRS, we understand that bureaucracies are callous creatures, capable of manipulation. In addition to deliberate misuse, closed intelligence agencies can make mistakes in surveilling legitimate targets, causing mountains of trouble. Consider Muslim names. Because of their commonness and the lack of standardized transliteration, they can befuddle scholars, let alone intelligence analysts, who seldom have fluency in Islamic languages. Although one is hard pressed to think of a case since 9/11 in which mistaken identity, or a willful or unintentional leak of intercept intelligence, immiserated an American citizen, these things can happen. NSA civilian employees, soldiers, FBI agents, CIA case officers, prosecutors, and our elected officials are not always angels. Even though encryption is mathematically easier to accomplish than decryption, the potential for abuse of digital communication is always there—all the more since few Americans resort to encryption of their everyday emails.

## THE NSA IMPLANTS ROUTERS WITH SURVEILLANCE TOOLS TO FACILITATE SPYING ON INTERNATIONAL USERS.

Darrell Etherington, [Contributor, Tech Crunch], "NSA Reportedly Intercepts and Alters Routers and Servers Exported from US To Facilitate Surveillance," Tech Crunch,<http://techcrunch.com/2014/05/13/nsa-reportedly-intercepts-and-alters-routers-and-servers-> exported-from-u-s-to-facilitate-surveillance/, May 13, 2014.

A new report from NSA leak story breaker Glenn Greenwald claims the U.S.-based National Security Agency actually intercepts and alters routers and server hardware exported from the

U.S. to implant them with surveillance tools to facilitate spying on international users. The source of the report is a June 2010 document from the NSA’s Access and Target Development department, which outlines the program in detail. Now, the NSA has responded with two official statements addressing the fresh accusations.¶ These devices, which are either received or intercepted by the NSA in the course of their export, could include routers, servers and “other computer network devices.” The agency is said to open them, implant beacons and other backdoor surveillance tools, and then repackage them complete with factory seals before sending them on to their final destination.

## THIS TYPE OF INVASION OF PRIVACY IS EXACTLY WHAT THE US HAS ACCUSED CHINA OF IN THE PAST.

Darrell Etherington, [Contributor, Tech Crunch], "NSA Reportedly Intercepts and Alters Routers and Servers Exported from US To Facilitate Surveillance," Tech Crunch,<http://techcrunch.com/2014/05/13/nsa-reportedly-intercepts-and-alters-routers-and-servers-> exported-from-u-s-to-facilitate-surveillance/, May 13, 2014.

If accurate, the report is especially damning because the U.S. government has, in the past, suggested that China-made network equipment has been intercepted and altered in exactly the same way. This has been used as grounds for encouraging U.S.-based firms to stick with hardware made by American-controlled companies, and to avoid network equipment built by Chinese corporations, including but not limited to Huawei and ZTE.

## THE SCOPE OF NSA SURVEILLANCE EXCEEDS ITS ABILITY TO ANALYZE IT.

David Cole, [Hon. George Mitchell professor in law and public policy at Georgetown University Law Center and is the legal affairs correspondent for the Nation.], "No Place to Hide by Glenn Greenwald, on the NSA's sweeping efforts to 'Know it All'," Washington Post, May 12, 2014.

Much has been written about the NSA’s omnivorous appetite for personal data — much of it by Greenwald for the Guardian and other outlets. In his new book, however, he offers a revealing and disturbing overview, illustrated by dozens of reproduced secret documents, of just how far the NSA has gone to achieve Alexander’s vision of collecting and knowing it all. Relying on newly disclosed and already disclosed documents, Greenwald shows that the scope of the NSA’s surveillance exceeds not only our imagination but also the agency’s capacity even to store, much less analyze, it all.

## THE NSA HAS ADMITTED THAT IT COLLECTS MUCH MORE DATA THAN IT CAN ANALYZE.

David Cole, [WP Contributor], "No Place to Hide by Glenn Greenwald, on the NSA's sweeping efforts to 'Know it All'," Washington Post, May 12, 2014.

In a one-month period last year, for example, a single unit of the NSA, the Global Access Operations unit, collected data on more than 97  billion e-mails and 124  billion phone calls from around the world; more than 3  billion of those calls and e-mails were collected as they passed

through the United States. As of 2012, the agency was processing more than 20 billion telecommunications per day. In a single month in 2011, the NSA collected 71 million calls and e- mails from Poland alone — not a major hub of terrorist activity, the last time I checked. The NSA has admitted that “it collects far more content than is routinely useful to analysts.” These numbers call to mind Sen. Everett Dirksen’s quip about government spending: “A billion here, a billion there, and pretty soon you’re talking about real money.”

*SOFT POWER*

## NSA SURVEILLANCE DEVASTATES OUR INTERNATIONAL CREDIBILITY

Chen, Xiangyang. [Research Fellow, China Institute of Contemporary International Relations].

"Strategic Impacts of the ‘Snowden Incident’ on International Relations," China US Focus. September 9, 2013, <http://www.chinausfocus.com/peace-security/strategic-impacts-of-the-> snowden-incident-on-international-relations/

Although the fireworks ignited by the “Snowden incident” have dimmed, its strategic impacts on international relations are only beginning to be felt. The incident is affecting the game theory among the world’s four leading powers of the US, China, Russia and European Union and leftwing forces in Latin America, involving state and non-state entities operating in cyber-space as well as the real world and reflecting a new characteristic of today’s multi-national politics. Due to the incident, three injuries have been inflicted on the US. First, it has seriously hurt the international image of America and somewhat weakened its “soft strength”. Secret operations such as “PRISM” have exposed the US double-standard on Internet security and online privacy, and proved beyond reasonable doubt the US hypocrisy over human rights, anti-terrorism and moral leadership. It also demonstrates how easy it is for the US not to match its own words with appropriate action and how porous its intelligence out-sourcing system is. There is no doubt the US will review its entire cyber-snooping system and make whatever improvement necessary. Just two years after WikiLeaks put thousands of classified telecommunications between Washington and US diplomatic missions around the world under the sun, the "Snowden incident" brought more of Washington's dark secrets into public view. Dealing such a heavy blow to the no-holds- barred global electronic surveillance franchise, the damage to US intelligence setup could be comparable to that of "9/11" to national security.

## SURVEILLANCE JUSTIFIES AUTHORITARIAN CRACKDOWNS AROUND THE WORLD

Rid, Thomas. [PhD., Reader in War Studies at King's College London]. "The Rest of the Snowden Files Should Be Destroyed," Slate. September 10, 2013,<http://www.slate.com/articles/technology/future_tense/2013/09/nsa_surveillance_the_rest_of_the>

\_snowden\_files\_should\_be\_destroyed.html

Meanwhile, thirdly, authoritarian states get a confidence boost. “Washington ate the dirt this time,” wrote China’s Global Times, an outlet sometimes called the Fox News of China. The U.S. administration “has long been trying to play innocent victim of cyberattacks” but now turned out to be “the biggest villain,” said Xinhua, the state-run news agency. This argument, of course, is hypocrisy. The National Security Agency is not spying in order to round up Obama's political opposition, and Government Communications Headquarters is not listening to Internet traffic to help London's banks—both of which stand in sharp contrast to China's own practices.

Nevertheless, Snowden's revelations make it easier for the world's authoritarian regimes to crush dissent at home. A fourth result: Internet governance is creaking. Diminishing America and Britain’s diplomatic and moral standing is threatening the multistakeholder approach, so far a guarantor for a free and open Internet. A patchwork of smaller, sovereign "Internets" is becoming more and more likely. As a result, the Internet could now become more authoritarian, not less.

*SURVEILLANCE STATE*

## THE INTERNET HAS BECOME A SURVEILLANCE STATE

Bruce Shneier 3/16, [security technologist and authors of "Liars and Outliers: Enabling the Trust Society Needs to Survive"], "The Internet is a surveillance state", CNN Opinion, [http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance/index.html.](http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance/index.html)

One: Some of the Chinese military hackers who were implicated in a broad set of attacks against the U.S. government and corporations were identified because they accessed Facebook from the same network infrastructure they used to carry out their attacks.¶ Two: Hector Monsegur, one of the leaders of the LulzSac hacker movement, was identified and arrested last year by the FBI. Although he practiced good computer security and used an anonymous relay service to protect his identity, he slipped up.¶ Bruce Schneier¶ And three: Paula Broadwell,who had an affair with CIA director David Petraeus, similarly took extensive precautions to hide her identity. She never logged in to her anonymous e-mail service from her home network. Instead, she used hotel and other public networks when she e-mailed him. The FBI correlated hotel registration data from several different hotels -- and hers was the common name.¶ The Internet is a surveillance state. Whether we admit it to ourselves or not, and whether we like it or not, we're being tracked all the time. Google tracks us, both on its pages and on other pages it has access to. Facebook does the same; it even tracks non-Facebook users. Apple tracks us on our iPhones and iPads. One reporter used a tool called Collusion to track who was tracking him; 105 companies tracked his Internet use during one 36-hour period.¶ Become a fan of CNNOpinion¶ Stay up to date on the latest opinion, analysis and conversations through social media. Join us at Facebook/CNNOpinion and follow us @CNNOpinion on Twitter. We welcome your ideas and comments. ¶ Increasingly, what we do on the Internet is being combined with other data about us. Unmasking Broadwell's identity involved correlating her Internet activity with her hotel stays. Everything we do now involves computers, and computers produce data as a natural by-product. Everything is now being saved and correlated, and many big-data companies make money by building up intimate profiles of our lives from a variety of sources.¶ News: Cyberthreats getting worse, House intelligence officials warn¶ Facebook, for example, correlates your online behavior with your purchasing habits offline. And there's more. There's location data from your cell phone, there's a record of your movements from closed-circuit TVs.¶ This is ubiquitous surveillance: All of us being watched, all the time, and that data being stored forever. This is what a surveillance state looks like, and it's efficient beyond the wildest dreams of George Orwell.¶ Sure, we can take measures to prevent this. We can limit what we search on Google from our iPhones, and instead use computer web browsers that allow us to delete cookies. We can use an alias on Facebook.

We can turn our cell phones off and spend cash. But increasingly, none of it matters.¶ There are simply too many ways to be tracked. The Internet, e-mail, cell phones, web browsers, social networking sites, search engines: these have become necessities, and it's fanciful to expect people to simply refuse to use them just because they don't like the spying, especially since the full extent of such spying is deliberately hidden from us and there are few alternatives being marketed by companies that don't spy.¶ This isn't something the free market can fix. We consumers have no choice in the matter. All the major companies that provide us with Internet services are interested in tracking us. Visit a website and it will almost certainly know who you are; there are lots of ways to be tracked without cookies. Cellphone companies routinely undo the web's privacy protection. One experiment at Carnegie Mellon took real-time videos of students on campus and was able to identify one-third of them by comparing their photos with publicly available tagged Facebook photos.¶ Maintaining privacy on the Internet is nearly impossible. If you forget even once to enable your protections, or click on the wrong link, or type the wrong thing, and you've permanently attached your name to whatever anonymous service you're using. Monsegur slipped up once, and the FBI got him. If the director of the CIA can't maintain his privacy on the Internet, we've got no hope.¶ In today's world, governments and corporations are working together to keep things that way. Governments are happy to use the data corporations collect -- occasionally demanding that they collect more and save it longer -- to spy on us. And

corporations are happy to buy data from governments. Together the powerful spy on the powerless, and they're not going to give up their positions of power, despite what the people want.¶ Fixing this requires strong government will, but they're just as punch-drunk on data as the corporations. Slap-on-the-wrist fines notwithstanding, no one is agitating for better privacy laws.¶ So, we're done. Welcome to a world where Google knows exactly what sort of porn you all like, and more about your interests than your spouse does. Welcome to a world where your cell phone company knows exactly where you are all the time. Welcome to the end of private conversations, because increasingly your conversations are conducted by e-mail, text, or social networking sites.¶ And welcome to a world where all of this, and everything else that you do or is done on a computer, is saved, correlated, studied, passed around from company to company without your knowledge or consent; and where the government accesses it at will without a warrant.¶ Welcome to an Internet without privacy, and we've ended up here with hardly a fight.

## SURVEILLANCE THAT UNDERMINES PRIVACY HURTS THE TECH INDUSTRY

John Grgurich, “NSA Snooping Isn’t Just a Privacy Problem,” *Fiscal Times* (Online), May 21st, 2014. URL = <<http://www.thefiscaltimes.com/Articles/2014/05/21/NSA-Snooping-Isn-t-Just-> Privacy-Problem>

The photo released with Glenn Greenwald’s new book No Place to Hide isn't what you'd expect an undercover National Security Agency operation to look like — four people with unimpressive physiques in a low-tech, poorly lit room pulling the packing tape off a Cisco Systems shipping box. Not exactly James Bond, but this shot and an accompanying image reportedly show NSA employees in the process of unpacking a Cisco router that's been covertly intercepted for the purpose of fitting it with "beacon firmware" that will later allow the NSA surreptitious entry.

The photos were part of a larger packet of revelatory materials released by Greenwald, the reporter who broke the Edward Snowden story. The fact that the NSA intercept shipments of such equipment wasn’t news, but the pictures were enough to provoke Cisco Chairman and CEO John Chambers to send a letter to President Obama expressing his frustration and concern: “We

simply cannot operate this way," Chambers wrote. "Our customers trust us to be able to deliver to

their doorsteps products that meet the highest standards of integrity and security.”

Cisco isn't the only tech company making its voice heard on how American surveillance practices may be bad for business. “People won’t use technology they don’t trust," Microsoft's general counsel Brad Smith is quoted as saying on Reform Government Surveillance, a website the tech industry is using to air related grievances. "Governments have put this trust at risk, and governments need to help restore it.”

On the same site, Yahoo! CEO Marissa Mayer had equally strong words for the president: "Recent revelations about government surveillance activities have shaken the trust of our users, and it is time for the United States government to act to restore the confidence of citizens around the world." And Facebook founder and CEO Mark Zuckerberg chimed in with: “Reports about government surveillance have shown there is a real need for greater disclosure and new limits on how governments collect information."

Cisco makes a good deal of the world's IT hardware. If businesses here and abroad start believing the NSA is routinely tampering with Cisco products, they may stop buying them. In announcing its quarterly results last week, Chambers revealed he thought this very effect was already at work. And if the NSA is getting to Cisco's products, it stands to reason other companies' IT products can be gotten to, as well, which could also put their reputations — and therefore their businesses — at risk.

*AT TERRORISM*

## NSA SURVEILLANCE IS NOT INSTRUMENTAL IN DISRUPTING TERRORIST PLOTS.

John Mueller [political scientist at Ohio state] and Mark G. Stewart [civil engineer at the University of Newcastle in Australia], "Three Questions about NSA Surveillance," Cato Institute, June 13, 2013.

There has been a lot of ominous stammering from Congress and the Obama administration about terrorist plots that have been disrupted by the programs. But thus far, only two concrete examples have been mentioned—not a great many for seven years of effort.¶ First, there have been suggestions that the NSA programs helped apprehend an American who had done surveillance work for the terrorist gunmen in Mumbai, India, in 2008. His efforts, however, were of limited importance to the event, and his eventual arrest didn’t prevent the attack.¶ The second was the 2009 Zazi case, in which three Afghan-Americans trained in Pakistan before returning to the United States and plotted to set off bombs in the New York subway system. Given the perpetrators’ limited capacities, it is questionable whether the plot would ever have succeeded.

Furthermore, the plot was disrupted not by NSA data-dredgers but by standard surveillance: British intelligence provided a hot tip about Zazi based on e-mail traffic to a known terrorist address—one that had long been watched.¶ At that point, U.S. authorities had good reason to put the plotters on their radar. Having NSA’s megadata collection may have been helpful, but it

seems scarcely to have been required. Actually, it is not clear that even the tip was necessary because the plotters foolishly called attention to themselves by using stolen credit cards to purchase large quantities of potential bomb material.

## CASE STUDIES INDICATE NSA PROGRAMS WERE NOT IMPORTANT.

John Mueller [political scientist at Ohio state] and Mark G. Stewart [civil engineer at the University of Newcastle in Australia], "Three Questions about NSA Surveillance," Cato Institute, June 13, 2013.

A set of case studies of the 53 post-9/11 plots by Islamist terrorists to damage targets in the United States suggests this is typical. Where the plots have been disrupted, as in the Zazi case, the task was accomplished by ordinary policing. The NSA programs scarcely come up at all.¶ When asked on Wednesday if the NSA’s data-gathering programs had been “critical” or “crucial” to disrupting terrorist threats, the agency’s head testified that in “dozens” of instances the database “helped” or was “contributing”—though he did seem to agree with the word “critical” at one point. He has promised to provide a list of those instances. The key issue for evaluating the programs, given their privacy implications, will be to determine not whether the huge database was helpful but whether it was necessary.

## DATA MINING WON’T WORK WITH TERRORISM.

Jim Harper, [director of information policy studies at the Cato Institute], "Officials Need to Come Clean on NSA Surveillance Activities," Cato Institute, June 6, 2013.

Data mining works with credit card fraud. There are thousands of examples per year from which to build models of what credit card fraud looks like in data. And the cost of getting it wrong is low. Credit card companies may call a customer or cause them a modest inconvenience by cancelling a card.¶ Data mining won’t work for terrorism because terrorism is too rare. There aren’t patterns reflecting terrorism planning or execution. Each plan and each attack, successful or unsuccessful, has been very different from the others. And the cost of false positives is high. Law enforcement personnel waste their time chasing false leads. Wrongly accused people are investigated, questioned, placed on no-fly lists or other derogatory lists, and sometimes people are wrongly arrested.

## SIMPLE TOOLS ARE MORE EFFECTIVE FOR COUNTERRORISM.

Erik J. Dahl, [Assistant Professor of National Security Affairs at the Naval Postgraduate School in Monterey, California], "Discussion Point: It's not Big Data, but Little Data, that Prevents Terrorist Attacks" National Consortium for the Study of Terrorism and Responses to Terrorism, July 25, 2015.

But another one of our findings is that the most effective tools in preventing terrorist attacks are relatively simple, old¶ fashioned police methods, such as the use of undercover officers, informants, and tips from the public. This is especially true¶ for domestic plots and attacks: of the 109 failed plots within the United States since 9/11, more than 75 percent were foiled at¶ least in part because of traditional law enforcement methods, and not—from what we can gather—from NSA surveillance.¶ Thus it is not surprising that government officials have said most of the 50 or so plots that have been foiled by the NSA¶ monitoring programs were overseas3. In other countries we can’t necessarily rely on local authorities, and spying—whether¶ conducted by the NSA or the CIA—is a critical tool for our national security. But here in the U.S., the most important terrorism¶ prevention tool remains the country’s 800,000 police officers, deputy sheriffs, and

other local law enforcement officials,¶ supported by members of the public who "see something

and say something," calling authorities when something doesn’t¶ look right.

## THERE'S NO EVIDENCE THE PROGRAM IS EFFECTIVE

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Needles Are Harder to Find in Bigger Haysticks," The New York Times. June 10, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-> surveillance-threat-real-or-imagined

Joshua, I agree with you that effectiveness matters. I can’t help but be skeptical, though. If these dragnet programs are effective, where’s the evidence? As you note, at least one of the success stories identified by anonymous intelligence officials—the story relating to Zazi—seems not to withstand scrutiny. Let’s also note that there’s no evidence the government has relied on evidence derived from these dragnet programs in criminal prosecutions. If these dragnet programs had been effective, wouldn’t we have seen at least a handful of criminal prosecutions? Of course intelligence surveillance has many purposes; gathering evidence of criminal activity is just one of them. Still, shouldn’t the apparent absence of any criminal prosecution make us question how necessary the programs really are? Lacking any more solid evidence of success, you fall back on the point that “the people who created and oversee” these programs “believe they are effective.” But unfortunately there are many reasons to question the trust you imply we should put in our national security agencies when they tell us, in essence, “we need more power to make you safe.”

## THE PROGRAM IS INEFFECTIVE AND UNDERMINES DEMOCRACY

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Needles Are Harder to Find in Bigger Haysticks," The New York Times. June 10, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-> surveillance-threat-real-or-imagined

It’s also worth remembering that the intelligence community’s biggest challenge has never been collecting information; the biggest challenge has always been making sense of it. Launching new programs to collect more information can be a good way to pad the pockets of defense contractors and data-miners, but, as many have noted, it isn’t usually a good way to identify terrorist threats. The analogy is now a bit threadbare, but it’s still useful: You don’t find needles by building bigger haystacks. After the NSA launched the warrantless wiretapping program, FBI agents repeatedly complained that they were drowning in useless information. (Eric Lichtblau wrote: “The torrent of tips led [the FBI] to few potential terrorists inside the country they did not know of from other sources and diverted agents from counterterrorism work they viewed as more productive.”). One of the 9/11 Commission’s most important observations was that the

intelligence community had information in the summer of 2001 that could have allowed it to prevent the 9/11 attacks. The problem wasn’t that it lacked information, but that it didn’t understand the information it had. Finally, “effectiveness” isn’t as simple as you make it out to be. A program can be effective in some very narrow sense but also seriously compromise our democracy over the long term. A program can be effective in some very narrow sense but also be fundamentally inconsistent with our values. Again, I agree that the effectiveness question is worth asking. But answering the effectiveness question isn’t as simple as asking whether these surveillance programs yielded useful information.

## THE PROGRAM ISN'T NECESSARY TO STOP TERRORISM

Bergen, Peter. [CNN's national security analyst and a director at the New America Foundation]. "Did NSA snooping stop 'dozens' of terrorist attacks?," CNN. June 18, 2013, <http://www.cnn.com/2013/06/17/opinion/bergen-nsa-spying/index.html>

Testifying before Congress on Wednesday, Gen. Keith Alexander, director of the National Security Agency, asserted that his agency's massive acquisition of U.S. phone data and the contents of overseas Internet traffic that is provided by American tech companies has helped prevent "dozens of terrorist events." On Thursday, Sens. Ron Wyden and Mark Udall, Democrats who both serve on the Senate Select Committee on Intelligence and have access to the nation's most sensitive secrets, released a statement contradicting this assertion. "Gen. Alexander's testimony yesterday suggested that the NSA's bulk phone records collection program helped thwart 'dozens' of terrorist attacks, but all of the plots that he mentioned appear to have been identified using other collection methods," the two senators said. Indeed, a survey of court documents and media accounts of all the jihadist terrorist plots in the United States since 9/11 by the New America Foundation shows that traditional law enforcement methods have overwhelmingly played the most significant role in foiling terrorist attacks. This suggests that the NSA surveillance programs are wide-ranging fishing expeditions with little to show for them.

## THE PROGRAM HAS NOT PREVENTED ANY ATTACKS

Bergen, Peter. [CNN's national security analyst and a director at the New America Foundation]. "Did NSA snooping stop 'dozens' of terrorist attacks?," CNN. June 18, 2013, <http://www.cnn.com/2013/06/17/opinion/bergen-nsa-spying/index.html>

Alexander promised during his congressional testimony that during this coming week more information would be forthcoming about how the NSA surveillance programs have prevented many attacks. A U.S. intelligence document provided to CNN by a congressional source over the weekend asserts that the dragnet of U.S. phone data and Internet information from overseas users "has contributed to the disruption of dozens of potential terrorist plots here in the homeland and in more than 20 countries around the world." The public record, which is quite rich when it comes to jihadist terrorism cases, suggests that the NSA surveillance yielded little of major value to prevent numerous attacks in the United States, but government officials may be able to point to a number of attacks that were averted overseas. That may not do much to dampen down the political firestorm that has gathered around the NSA surveillance programs. After all, these have been justified because they have supposedly helped to keep Americans safe at home.

## ATTACKS THAT HAVE BEEN PREVENTED WEREN'T BECAUSE OF THE NSA

Bergen, Peter. [CNN's national security analyst and a director at the New America Foundation]. "Did NSA snooping stop 'dozens' of terrorist attacks?," CNN. June 18, 2013, <http://www.cnn.com/2013/06/17/opinion/bergen-nsa-spying/index.html>

Homegrown jihadist extremists have mounted 42 plots to conduct attacks within the United States since 2001. Of those plots, nine involved an actual terrorist act that was not prevented by any type of government action, such as the failed attempt by Faisal Shahzad to blow up a car bomb in Times Square on May 1, 2010. Of the remaining 33 plots, the public record shows that at least 29 were uncovered by traditional law enforcement methods, such as the use of informants, reliance on community tips about suspicious activity and other standard policing practices. Informants have played a critical role in preventing more than half of the plots by homegrown jihadist extremists since the 9/11 attacks, according to New America Foundation data. For instance, a group of Muslims from the Balkans living in southern New Jersey who were virulently opposed to the Iraq War told a government informant in 2007 they were plotting to kill soldiers stationed at the nearby Fort Dix army base. Other investigations have relied on tips to law enforcement. Saudi student Khalid Aldawsari's plot to attack a variety of targets in Texas in 2011, including President George W. Bush's home in Dallas, was foiled when a company reported his attempt to buy chemicals suitable for making explosives. Standard police work has also stopped plots. Kevin Lamar James, a convert to Islam, formed a group dedicated to holy war while he was jailed in California's Folsom Prison during the late 1990s. James' crew planned to attack a U.S. military recruiting station in Los Angeles on the fourth anniversary of 9/11 as well as a synagogue a month later.

## TERRORIST ATTACKS CAN BE PREVENTED OTHER WAYS

Mueller, John. [Professor of International Relations at Ohio State University]. AND Stewart, Mark

G. [civil engineer at the University of Newcastle in Australia and a visiting fellow at Cato]. "3 Questions About NSA Surveillance," The Chronicle of Higher Education. June 13, 2013, https://chronicle.com/blogs/conversation/2013/06/13/3-questions-about-nsa-surveillance/

A set of case studies of the 53 post-9/11 plots by Islamist terrorists to damage targets in the United States suggests this is typical. Where the plots have been disrupted, as in the Zazi case, the task was accomplished by ordinary policing. The NSA programs scarcely come up at all.

When asked on Wednesday if the NSA’s data-gathering programs had been “critical” or “crucial” to disrupting terrorist threats, the agency’s head testified that in “dozens” of instances the database “helped” or was “contributing”—though he did seem to agree with the word “critical” at one point. He has promised to provide a list of those instances. The key issue for evaluating the programs, given their privacy implications, will be to determine not whether the huge database was helpful but whether it was necessary.

## EMPIRICAL EXAMPLES PROVE THE PROGRAM IS NOT BENEFICIAL

Mueller, John. [Professor of International Relations at Ohio State University]. AND Stewart, Mark

G. [civil engineer at the University of Newcastle in Australia and a visiting fellow at Cato]. "3 Questions About NSA Surveillance," The Chronicle of Higher Education. June 13, 2013, https://chronicle.com/blogs/conversation/2013/06/13/3-questions-about-nsa-surveillance/

There has been a lot of ominous stammering from Congress and the Obama administration about terrorist plots that have been disrupted by the programs. But thus far, only two concrete examples have been mentioned—not a great many for seven years of effort. First, there have been suggestions that the NSA programs helped apprehend an American who had done surveillance work for the terrorist gunmen in Mumbai, India, in 2008. His efforts, however, were of limited importance to the event, and his eventual arrest didn’t prevent the attack. The second was the 2009 Zazi case, in which three Afghan-Americans trained in Pakistan before returning to the United States and plotted to set off bombs in the New York subway system. Given the perpetrators’ limited capacities, it is questionable whether the plot would ever have succeeded.

Furthermore, the plot was disrupted not by NSA data-dredgers but by standard surveillance: British intelligence provided a hot tip about Zazi based on e-mail traffic to a known terrorist address—one that had long been watched. At that point, U.S. authorities had good reason to put the plotters on their radar. Having NSA’s megadata collection may have been helpful, but it seems scarcely to have been required. Actually, it is not clear that even the tip was necessary because the plotters foolishly called attention to themselves by using stolen credit cards to purchase large quantities of potential bomb material.

## TERRORISTS ARE ADAPTING TO AVOID SURVEILLANCE

Dozier, Kimberly. [staff writer at the Associated Press]. "AL-QAIDA SAID TO BE CHANGING ITS WAYS AFTER LEAKS," The Associated Press. July 26, 2013, <http://bigstory.ap.org/article/al-> qaida-said-be-changing-its-ways-after-leaks

Two U.S. intelligence officials say members of virtually every terrorist group, including core al- Qaida members, are attempting to change how they communicate, based on what they are reading in the media, to hide from U.S. surveillance. It is the first time intelligence officials have described which groups are reacting to the leaks. The officials spoke anonymously because they were not authorized to speak about the intelligence matters publicly. The officials wouldn't go into details on how they know this, whether it's terrorists switching email accounts or cellphone providers or adopting new encryption techniques, but a lawmaker briefed on the matter said al- Qaida's Yemeni offshoot, al-Qaida in the Arabian Peninsula, has been among the first to alter how it reaches out to its operatives. The lawmaker spoke anonymously because he would not, by name, discuss the confidential briefing. Shortly after Edward Snowden leaked documents about the secret NSA surveillance programs, chat rooms and websites used by like-minded extremists and would-be recruits advised users how to avoid NSA detection, from telling them not to use their real phone numbers to recommending specific online software programs to keep spies from tracking their computers' physical locations.

## THE PROGRAM IS A HUGE WASTE OF TAX DOLLARS

Mueller, John. [Professor of International Relations at Ohio State University]. AND Stewart, Mark

G. [civil engineer at the University of Newcastle in Australia and a visiting fellow at Cato]. "3 Questions About NSA Surveillance," The Chronicle of Higher Education. June 13, 2013, https://chronicle.com/blogs/conversation/2013/06/13/3-questions-about-nsa-surveillance/

After 9/11, U.S. intelligence concluded that there were thousands of Al Qaeda operatives in the country. That perspective impelled a vast and hasty increase in spending on intelligence and policing, and at least 263 military and intelligence agencies have been created or reorganized. For its part, the Department of Homeland Security has set up a vast array of “fusion centers” to police terrorism, but is unable to determine how much they cost. It estimates that somewhere between $289-million and $1.4-billion were awarded to them from 2003 to 2010—a gap of over a billion dollars that is impressive even by Washington standards. As it turned out, the number of Al Qaeda operatives actually in the United States registered at zero or nearly so, and the threat of terrorism in the country proved to be far more limited than initially feared. Accordingly, there might logically have been some judicious cutbacks in the funds devoted to the expensive quest to find terrorists who mostly didn’t exist—a process some in the FBI call “ghost chasing.” However, the reaction has continually been to expand the enterprise, searching for the needle by adding more and more hay. Far overdue are extensive openly published studies that rationally evaluate homeland-security expenditures. The NSA’s formerly secret surveillance programs have been

part of the expansionary process. If they have done little to prevent terrorist attacks in the United States, and if we are now having what President Obama has characterized as a “healthy” debate about the programs, it seems reasonable to suggest that the debaters should at least be supplied with information about how much the programs cost. Knowing the cost would scarcely help the terrorists. It might, however, amaze American taxpayers. Perhaps that’s another reason the programs have been kept secret.

## THE TIPS PROGRAM WILL MAKE US A NATION OF SUSPECTS.

Charles V. Pena, [Senior defense policy analyst at the Cato Institute], "Information Awareness Office Makes Us a Nation of Suspects," Cato Institute, November 29, 2002.

The TIPS (Terrorist Information and Prevention Service) program proposed by the Justice Department that would have made us a nation of snitches was bad enough. Total Information Awareness is much worse. It will make us a nation of suspects.¶ Call it what you want, but Total Information Awareness is the federal government creating a surveillance state to spy on its own citizenry. Of course, the rationale for such draconian action is that it will help catch would-be terrorists before they inflict harm on innocent Americans. This preys on the public’s new sense of vulnerability and places safety above liberty. As Benjamin Franklin said: “They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.”

## TIPS IS ESSENTIALLY HIGH-TECH MCCARTHYISM.

Charles V. Pena, [Senior defense policy analyst at the Cato Institute], "Information Awareness Office Makes Us a Nation of Suspects," Cato Institute, November 29, 2002.

Total Information Awareness is a fishing expedition that will cast a net over all Americans. Indeed, data mining currently targets millions of Americans as potential customers for a variety of products and services. Yet how many people - who are supposed to fit the profile of a likely customer - receive unwanted telephone, mail, and electronic solicitations? Telemarketers and junk mail are an inconvenience and annoyance. Now imagine that the computers are correlating data to create lists of would-be terrorists. The result could amount to high-tech McCarthyism.¶ How many innocent Americans will be wrongfully accused? How many will be incarcerated, perhaps indefinitely, and possibly denied their Constitutional rights - including access to legal counsel - if declared “enemy combatants”? How many will share the same fate as Richard Jewell, who was suspected of the Atlanta Olympic Park bombing? It turned out that he actually acted to thwart the bombing. But because he was the sole focus of the FBI’s investigation and the subject of intense media scrutiny his life was nonetheless ruined, without so much as an apology from the federal government.